# ENDPOINT SECURITY

FÜR MAC

## Benutzerhandbuch

(für Produktversion 6.0 und höher)

Klicken Sie hier, um die neueste Version dieses Dokuments herunterzuladen

**©ESET, spol. s.r.o.**
ESET Endpoint Security wurde entwickelt von ESET, spol. s r.o.
Weitere Informationen finden Sie unter www.eset.com.
Alle Rechte vorbehalten. Kein Teil dieser Dokumentation darf ohne schriftliche Einwilligung des Verfassers reproduziert, in einem Abrufsystem gespeichert oder in irgendeiner Form oder auf irgendeine Weise weitergegeben werden, sei es elektronisch, mechanisch, durch Fotokopien, Aufnehmen, Scannen oder auf andere Art.
ESET, spol. s r.o. behält sich das Recht vor, ohne vorherige Ankündigung an jeder der hier beschriebenen Software-Produkte Änderungen vorzunehmen.

Support: www.eset.com/support

Stand 25. 8. 2015

# Inhalt


1. ESET Endpoint Security....4
1.1 Neuerungen in Version 6....4
1.2 Systemanforderungen....4
2. Benutzerverbindungen über ESET Remote Administrator....4
2.1 ESET Remote Administrator-Server....5
2.2 Web-Konsole....5
2.3 Proxy....5
2.4 Agent....6
2.5 RD Sensor....6
3. Installation....6
3.1 Standardinstallation....7
3.2 Benutzerdefinierte Installation....7
3.3 Remoteinstallation....8
3.3.1 Ein Remoteinstallationspaket erstellen....8
3.3.2 Remoteinstallation auf den Zielrechnern....9
3.3.3 Remote-Deinstallation....9
3.3.4 Remote-Upgrade....9
4. Produktaktivierung....9
5. Deinstallation....10
6. Übersicht....10
6.1 Tastaturbefehle....10
6.2 Überprüfen der Funktionsfähigkeit des Systems....11
6.3 Vorgehensweise bei fehlerhafter Ausführung des Programms....11
7. Computerschutz....11
7.1 Viren- und Spyware-Schutz....11
7.1.1 Allgemein....11
7.1.1.1 Ausschlussfilter....12
7.1.2 Systemstart-Schutz....12
7.1.3 Echtzeit-Dateischutz....12
7.1.3.1 Scannen bei (Scannen bei Ereignis)....12
7.1.3.2 Erweiterte Optionen für Scans....12
7.1.3.3 Wann sollten die Einstellungen für den Echtzeit-Dateischutz geändert werden?....13
7.1.3.4 Echtzeit-Dateischutz prüfen....13
7.1.3.5 Vorgehensweise bei fehlerhaftem Echtzeit-Dateischutz....13
7.1.4 On-Demand-Scan....14
7.1.4.1 Scanmethode....14
7.1.4.1.1 Smart-Scan....14
7.1.4.1.2 Benutzerdefinierter Scan....14
7.1.4.2 Zu scannende Objekte....14
7.1.4.3 Scanprofile....15
7.1.5 Einstellungen für ThreatSense....15
7.1.5.1 Objekte....16
7.1.5.2 Optionen....16
7.1.5.3 Säubern....16
7.1.5.4 Ausschlussfilter....17
7.1.5.5 Grenzen....17
7.1.5.6 Weitere....17
7.1.6 Eingedrungene Schadsoftware wurde erkannt....18
7.2 Web- und E-Mail-Schutz....18
7.2.1 Web-Schutz....18
7.2.1.1 Ports....18
7.2.1.2 Aktiver Modus....19
7.2.1.3 URL-Listen....19
7.2.2 E-Mail-Schutz....19
7.2.2.1 Prüfen des POP3-Protokolls....20
7.2.2.2 Prüfen des IMAP-Protokolls....20
7.3 Phishing-Schutz....20
8. Firewall....20
8.1 Filtermodi....20
8.2 Firewall-Regeln....21
8.2.1 Erstellen neuer Regeln....21
8.3 Firewall-Zonen....22
8.4 Firewall-Profile....22
8.5 Firewall-Logs....22
9. Medienkontrolle....22
9.1 Regel-Editor....22
10. Web-Kontrolle....24
11. Tools....24
11.1 Log-Dateien....24
11.1.1 Log-Wartung....25
11.1.2 Log-Filter....26
11.2 Taskplaner....26
11.2.1 Erstellen von Tasks....26
11.2.2 Erstellen eines benutzerdefinierten Tasks....27
11.3 Live Grid....27
11.3.1 Verdächtige Dateien....28
11.4 Quarantäne....28
11.4.1 Quarantäne für Dateien....28
11.4.2 Wiederherstellen einer Datei aus der Quarantäne....29
11.4.3 Einreichen von Dateien aus der Quarantäne....29
11.5 Berechtigungen....29
11.6 Präsentationsmodus....29
11.7 Ausgeführte Prozesse....30
12. Benutzeroberfläche....31
12.1 Warnungen und Benachrichtigungen....31
12.1.1 Erweiterte Einstellungen für Warnungen und Benachrichtigungen....31
12.2 Kontextmenü....31
13. Update....31
13.1 Einstellungen für Updates....32
13.1.1 Erweiterte Einstellungen....32
13.2 So erstellen Sie Update-Tasks....33
13.3 Upgrade auf ein neues Build....33
13.4 Systemupdates....33
14. Allgemein....34
14.1 Einstellungen importieren/exportieren....34
14.1.1 Einstellungen importieren....34
14.1.2 Einstellungen exportieren....34
14.2 Einstellungen für den Proxyserver....34
14.3 Freigegebener lokaler Cache....35

# 1. ESET Endpoint Security

ESET Endpoint Security 6 ist ein neuer Ansatz für vollständig integrierte Computersicherheit. Die neueste Version des Scanmoduls ThreatSense® bietetin Verbindung mit der Personal Firewall eine schnelle und sichere Lösung, die Sicherheit Ihres Computers zu gewährleisten. Das Ergebnis ist ein intelligentes System, das permanent vor Angriffen und bösartiger Software schützt, die Ihren Computer gefährden können.

ESET Endpoint Security 6 ist eine umfassende Sicherheitslösung und das Produkt unserer langfristigen Bemühung, maximalen Schutz bei minimaler Systembelastung zu bieten. Mithilfe der auf künstlicher Intelligenz basierenden Spitzentechnologien kann das Eindringen von Viren, Spyware, Trojanern, Würmern, Adware, Rootkits und anderer durch das Internet übertragener Angriffe aktiv verhindert werden, ohne dass die Systemleistung beeinträchtigt oder Ihr Computer vom Netz getrennt würde.

ESET Endpoint Security 6 wurde speziell für die Nutzung auf Workstations in kleineren Unternehmen entwickelt. In Verbindung mit ESET Remote Administrator 6 können Sie damit eine beliebige Anzahl von Client-Workstations verwalten, Richtlinien und Regeln anwenden, Erkennungen überwachen und von einem beliebigen Computer im Netzwerk Änderungen verwalten.

### 1.1 Neuerungen in Version 6

Die grafische Benutzeroberfläche von ESET Endpoint Security wurde komplett neu gestaltet, um eine verbesserte Sichtbarkeit und eine intuitivere Bedienung zu ermöglichen. Zu den zahlreichen Verbesserungen in Version 6 gehören:

- **Firewall** - Sie können Firewall-Regeln jetzt direkt im Log oder im IDS-Benachrichtigungsfenster erstellen und Netzwerkschnittstellen Profile zuweisen.
- **Web-Kontrolle** - Sperrt Webseiten, die möglicherweise unerlaubte oder ungeeignete Inhalte enthalten.
- **Web-Schutz** - Der Web-Schutz überwacht die Kommunikation zwischen Webbrowsern und Remoteservern.
- **E-Mail-Schutz** - dient der Überwachung eingehender E-Mails, die mit dem POP3- oder IMAP-Protokoll übertragen werden.
- **Phishing-Schutz** - Schützt Sie vor Versuchen unseriöser Webseiten, an Passwörter und andere sicherheitsrelevante Informationen zu gelangen, indem sie sich als seriöse Webseiten ausgeben.
- **Medienkontrolle** – Mit dieser Funktion können Sie Medien bzw. Geräte scannen oder sperren oder erweiterte Filter- und/oder Berechtigungseinstellungen anpassen und definieren, wie ein Benutzer auf externe Geräte zugreifen und mit ihnen arbeiten kann. Diese Funktion ist ab Produktversion 6.1 verfügbar.
- **Präsentationsmodus** - ermöglicht das Ausführen von ESET Endpoint Security im Hintergrund und unterdrückt Popup-Fenster und geplante Tasks.
- **Freigegebener lokaler Cache** – Die Funktion des freigegebenen lokalen Cache ermöglicht ein schnelleres Scannen in virtuellen Umgebungen.

### 1.2 Systemanforderungen

Um mit ESET Endpoint Security eine optimale Leistung zu erreichen, sollten die folgenden Hardware- und Softwareanforderungen erfüllt sein:

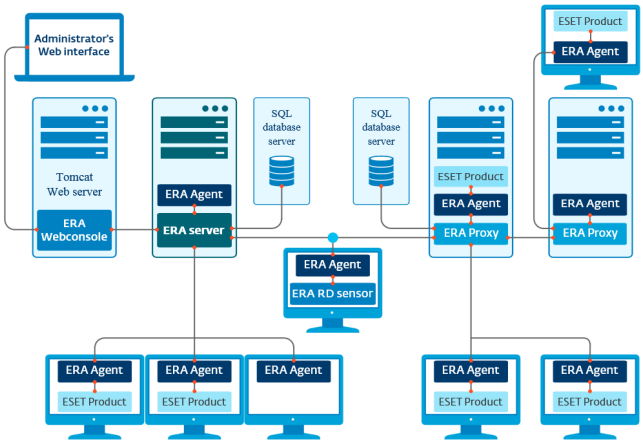
| | Systemanforderungen: |
|---|---|
| Prozessorarchitektur | Intel 32-bit, 64-bit |
| Betriebssystem | Mac OS X 10.6 und höher<br><br>**HINWEIS:** Clients, die unter Mac OS X 10.6 ausgeführt werden, können nicht mit ESET Remote Administrator 6.x verwaltet werden. |
| Speicher | 300 MB |
| Freier Speicherplatz | 200 MB |

# 2. Benutzerverbindungen über ESET Remote Administrator

Mit ESET Remote Administrator (ERA) 6 können Sie ESET-Produkte in einer Netzwerkumgebung von einem zentralen Standort aus verwalten. Mit dem Task-Management-System von ESET Remote Administrator können Sie ESET-Sicherheitslösungen auf Remotecomputern installieren und schnell auf neue Probleme und Bedrohungen reagieren. ESET Remote Administrator bietet keinen Schutz vor Schadcode selbst, sondern stützt sich hierzu auf die auf jedem Client installierte ESET-Sicherheitslösung.

ESET-Sicherheitslösungen unterstützen Netzwerke, die verschiedene Plattformtypen umfassen. Ihr Netzwerk kann aus einer Kombination aktueller Microsoft-, Linux- und OS X-Betriebssysteme und Betriebssysteme für mobile Geräte (Mobiltelefone und Tablets) bestehen.

In der nachstehenden Abbildung sehen Sie eine Beispielarchitektur eines Netzwerks mit ESET-Sicherheitslösungen, die über ERA verwaltet werden:




**HINWEIS:** Weitere Informationen finden Sie in der ESET Remote Administrator-Onlinedokumentation.

## 2.1 ESET Remote Administrator-Server

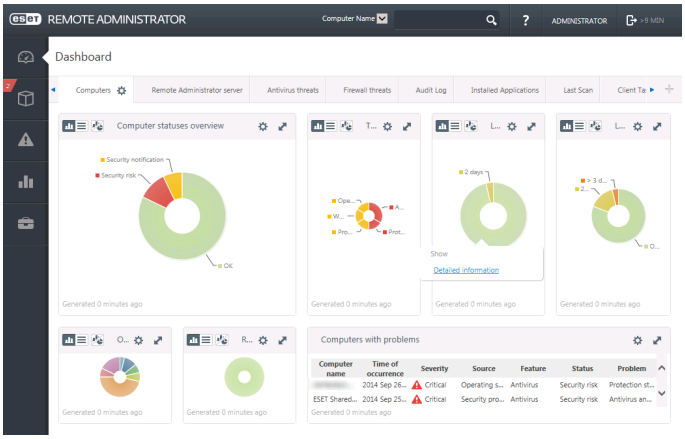
ESET Remote Administrator-Server ist eine Hauptkomponente von ESET Remote Administrator. Diese Komponente verarbeitet alle Daten von den Clients, die über den ESET-Agenten 6 mit dem Server kommunizieren. Der ESET-Agent erleichtert die Kommunikation zwischen Client und Server. Daten wie Client-Logs, Konfigurationseinstellungen oder Agentreplikationen werden in einer Datenbank gespeichert, auf die ERA zur Berichterstellung zugreift.

Zur ordnungsgemäßen Verarbeitung der Daten benötigt der ERA-Server eine stabile Verbindung zum Datenbankserver. Zum Zwecke der Leistungsoptimierung wird empfohlen, den ERA-Server und die Datenbank auf separaten Servern zu installieren. Der Computer, auf dem der ERA-Server installiert wird, muss so konfiguriert sein, dass alle Agent-/Proxy-/RD Sensor-Verbindungen, welche anhand von Zertifikaten überprüft werden, akzeptiert werden. Nachdem der ERA-Server installiert ist, können Sie die ERA-Web-Konsole 5 öffnen und hier Arbeitsstationen verwalten, auf denen ESET-Lösungen installiert sind.

## 2.2 Web-Konsole

Die **ERA-Web-Konsole** ist eine webbasierte Benutzeroberfläche, in der Sie Daten vom ERA-Server 5 anzeigen und die ESET-Sicherheitslösungen in Ihrem Netzwerk verwalten können. Der Zugriff auf die Web-Konsole erfolgt über einen Browser. Sie bietet eine Übersicht über den Status der Clients im Netzwerk und kann zur Remote-Bereitstellung von ESET-Lösungen auf unverwalteten Computern verwendet werden. Wahlweise können Sie den Zugriff über das Internet auf den Webserver zulassen. So können Sie ESET Remote Administrator von nahezu jedem beliebigen Standort und Gerät aus verwenden.

Dashboard der Web-Konsole:




Oben in der Web-Konsole befindet sich das **Schnellsuche**-Tool. Wählen Sie im Dropdownmenü entweder **Computername**, **IPv4-/IPv6-Adresse** oder **Bedrohungsname** aus und geben Sie im Textfeld eine Zeichenfolge für die Suche ein. Klicken Sie dann auf das Lupensymbol und drücken Sie die **Eingabetaste**, um die Suche auszuführen. Sie werden zum Bereich „Gruppen“ geleitet, wo das Suchergebnis angezeigt wird.

## 2.3 Proxy

Der **ERA-Proxy** ist ein weiterer Bestandteil von ESET Remote Administrator, der zwei Hauptzwecke erfüllt. In einem mittelgroßen Netzwerk oder Unternehmensnetzwerk mit vielen Clients (beispielsweise 10.000 Clients oder mehr) können Sie mit einem ERA-Proxy die Last zwischen mehreren ERA-Proxys verteilen und so den primären ERA-Server 5 entlasten. Sie können den ERA-Proxy außerdem für Verbindungen zu entfernt liegenden Büros mit schwacher Bandbreite einsetzen. In diesem Fall wird der ERA-Agent auf den Clients nicht direkt mit dem ERA-Hauptserver verbunden, sondern kommuniziert über den ERA-Proxy, der sich im gleichen lokalen Netzwerk wie der Client befindet. Diese Konfiguration reduziert die Last auf der Netzwerkverbindung zum Zweigstellenbüro. Der ERA-Proxy nimmt

Verbindungen von allen lokalen ERA-Agenten an, kompiliert die empfangenen Daten und lädt sie zum primären ERA-Server (oder zu einem anderen ERA-Proxy) hoch. Auf diese Weise ist im Netzwerk Platz für mehr Clients, ohne dass die Leistungsfähigkeit des Netzwerks und der Datenbankabfragen beeinträchtigt wird.

Je nach Netzwerkkonfiguration kann ein ERA-Proxy eine Verbindung zu einem anderen ERA-Proxy und anschließend zum ERA-Server herstellen.

Damit der ERA-Proxy ordnungsgemäß funktioniert, muss auf dem Hostcomputer, auf dem sich der ERA-Proxy befindet, ein ESET-Agent installiert sein, und er muss mit der oberen Ebene (entweder dem ERA-Server oder, sofern vorhanden, dem oberen ERA-Proxy) des Netzwerks verbunden sein.

### 2.4 Agent

Der **ERA-Agent** ist eine wichtige Komponente von ESET Remote Administrator. Der Agent dient der Kommunikation zwischen den ESET-Sicherheitslösungen auf den Clientcomputern (z. B. ESET Endpoint Security) und dem ERA-Server. Dank dieser Kommunikation können Sie ESET-Sicherheitslösungen auf Remoteclients von einem zentralen Standort aus verwalten. Der Agent erfasst Informationen vom Client und sendet sie an den Server. Wenn der Server einen Task an einen Client sendet, wird der Task an den Agenten übermittelt, der wiederum mit dem Client kommuniziert. Der gsamte Netzwerkverkehr findet zwischen dem Agenten und dem oberen Teil des ERA-Netzwerks (Server und Proxy) statt.

Der ESET-Agent stellt mit einer der folgenden drei Methoden eine Verbindung zum Server her:

1. Der Agent des Client ist direkt mit dem Server verbunden.
2. Der Agent des Client ist über einen Proxy mit dem Server verbunden.
3. Der Agent des Client ist über mehrere Proxys mit dem Server verbunden.

Der ESET-Agent kommuniziert mit ESET-Lösungen auf einem Client, sammelt Daten aus Programmen auf diesem Client und leitet vom Server erhaltene Konfigurationsdaten an den Client weiter.

**HINWEIS:** Der ESET-Proxy verfügt über einen eigenen Agenten, der alle Kommunikationstasks zwischen Clients, anderen Proxys und dem Server abwickelt.

### 2.5 RD Sensor

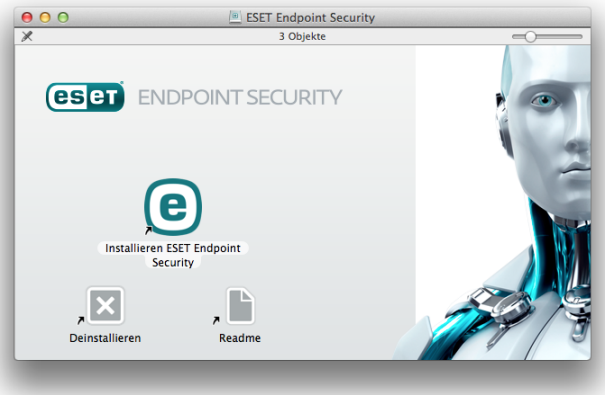
**RD (Rogue Detection) Sensor** ist eine Komponente von ESET Remote Administrator, die das Netzwerk nach Computern durchsucht. Auf diese Weise können neue Computer bequem und ohne manuelles Suchen zu ESET Remote Administrator hinzugefügt werden. Jeder im Netzwerk gefundene Computer wird in der Web-Konsole angezeigt und der Standardgruppe „Alle“ hinzugefügt. Anschließend können Sie Aktionen an den einzelnen Clientcomputern durchführen.

RD Sensor ist ein passives Überwachungstool, das Computer erkennt, die im Netzwerk vorhanden sind, und Informationen über diese Computer an den ERA-Server sendet. Der ERA-Server bewertet dann, ob die im Netzwerk gefundenen Computer unbekannt oder bereits verwaltet sind.

## 3. Installation

Das Installationsprogramm für ESET Endpoint Security für Mac kann auf zwei verschiedene Arten gestartet werden:

- Wenn Sie die Installation über eine Installations-CD/-DVD ausführen möchten, legen Sie die Disc in das CD-/DVD-ROM-Laufwerk ein und doppelklicken Sie auf das ESET Endpoint Security-Installationssymbol, um das Installationsprogramm zu starten.
- Wenn Sie zur Installation eine heruntergeladene Datei verwenden, starten Sie das Installationsprogramm durch einen Doppelklick auf die Datei.




Der Installationsassistent führt Sie durch die grundlegende Einrichtung. Zu Beginn der Installation prüft das Installationsprogramm automatisch online auf die neueste Produktversion. Wird eine neuere Version gefunden, erhalten Sie die Möglichkeit, vor dem Fortsetzen der Installation die neueste Version herunterzuladen.

Nachdem Sie der Endbenutzer-Lizenzvereinbarung (EULA) zugestimmt haben, können Sie eine der folgenden Installationsarten wählen:

- Standardinstallation 7
- Benutzerdefinierte Installation 7
- Remoteinstallation 8

## 3.1 Standardinstallation

Bei der Standardinstallation wird eine Konfiguration verwendet, die für die Anforderungen der meisten Benutzer geeignet ist. Sie bietet optimale Sicherheit und gleichzeitig gute Systemleistung. Die Standardinstallation wird daher empfohlen, wenn Sie keine speziellen Anforderungen an die Konfiguration haben.

**ESET Live Grid**
Durch das ESET Live Grid-Frühwarnsystem ist ESET beim Auftauchen neuer Infiltrationen immer auf dem neuesten Stand und kann seine Kunden schneller schützen. Das System ermöglicht das Übermitteln von Informationen zu neuen Bedrohungen an das ESET-Virenlabor. Hier werden die Bedrohungen analysiert, verarbeitet und zur Signaturdatenbank hinzugefügt. Klicken Sie auf **Einstellungen**, um Einstellungen für das Einsenden verdächtiger Dateien festzulegen. Weitere Informationen finden Sie im Abschnitt Live Grid 27.

**Eventuell unerwünschte Anwendungen**
Im letzten Schritt der Installation wird die Erkennung für **Eventuell unerwünschte Anwendungen** konfiguriert. Bei eventuell unerwünschten Anwendungen handelt es sich um Programme, die zwar nicht unbedingt Sicherheitsrisiken in sich bergen, jedoch negative Auswirkungen auf das Verhalten Ihres Computers haben können. Diese Anwendungen sind oft mit anderen Programmen gebündelt und daher während des Installationsvorgangs schwer erkennbar. Obwohl bei solchen Anwendungen während der Installation gewöhnlich eine Benachrichtigung angezeigt wird, können sie auch leicht ohne Ihre Zustimmung installiert werden.

Nach der Installation von ESET Endpoint Security sollte der Computer auf Schadcode gescannt werden. Klicken Sie dazu im Hauptprogrammfenster auf **Computer scannen** und dann auf **Smart-Scan**. Nähere Informationen zum On-Demand-Scan finden Sie im Abschnitt On-Demand-Scan 14.

## 3.2 Benutzerdefinierte Installation

Die benutzerdefinierte Installation eignet sich für fortgeschrittene Benutzer, die während der Installation die erweiterten Einstellungen ändern möchten.

**Programmkomponenten**
ESET Endpoint Security ermöglicht die Installation des Produkts ohne bestimmte Kernkomponenten (zum Beispiel ohne den Web- und E-Mail-Schutz). Deaktivieren Sie das Kontrollkästchen neben einer Produktkomponente, um sie aus der Installation zu entfernen.

**Proxyserver**
Wenn Sie einen Proxyserver verwenden, können Sie die entsprechenden Parameter festlegen, indem Sie die Option **Ich nutze einen Proxyserver** auswählen. Geben Sie im nächsten Fenster unter **Adresse** die IP-Adresse oder URL des Proxyservers ein. Geben Sie dann im Feld „Port“ den Port an, über den Verbindungen auf dem Proxyserver eingehen (standardmäßig 3128). Falls für den Proxyserver eine Authentifizierung erforderlich ist, geben Sie einen gültigen **Benutzernamen** und das **Passwort** ein. Wenn Sie keinen Proxyserver verwenden, wählen Sie die Option **Keinen Proxyserver verwenden**. Wenn Sie unsicher sind, ob Sie einen Proxyserver verwenden, können Sie Ihre aktuellen Systemeinstellungen verwenden. Wählen Sie dazu **Systemeinstellungen verwenden (empfohlen)**.

**Berechtigungen**
Im nächsten Schritt können Sie privilegierte Benutzer oder Gruppen definieren, die berechtigt sind, die Programmkonfiguration zu ändern. Wählen Sie links aus der Benutzerliste die Benutzer aus und fügen Sie sie über die Schaltfläche **Hinzufügen** zur Liste **Privilegierte Benutzer** hinzu. Um alle Systembenutzer anzuzeigen, wählen Sie die Option **Alle Benutzer anzeigen** aus. Wenn Sie die Liste der privilegierten Benutzer leer lassen, werden alle Benutzer als privilegiert betrachtet.

**ESET Live Grid**
Durch das ESET Live Grid-Frühwarnsystem ist ESET beim Auftauchen neuer Infiltrationen immer auf dem neuesten Stand und kann seine Kunden schneller schützen. Das System ermöglicht das Übermitteln von Informationen zu neuen Bedrohungen an das ESET-Virenlabor. Hier werden die Bedrohungen analysiert, verarbeitet und zur Signaturdatenbank hinzugefügt. Klicken Sie auf **Einstellungen**, um Einstellungen für das Einsenden verdächtiger Dateien festzulegen. Weitere Informationen finden Sie im Abschnitt Live Grid 27.

**Eventuell unerwünschte Anwendungen**
Im nächsten Schritt der Installation wird die Prüfung auf **Eventuell unerwünschte Anwendungen** konfiguriert. Bei eventuell unerwünschten Anwendungen handelt es sich um Programme, die zwar nicht unbedingt Sicherheitsrisiken in sich bergen, jedoch negative Auswirkungen auf das Verhalten Ihres Computers haben können. Diese Anwendungen sind oft mit anderen Programmen gebündelt und daher während des Installationsvorgangs schwer erkennbar. Obwohl bei solchen Anwendungen während der Installation gewöhnlich eine Benachrichtigung angezeigt wird, können sie auch leicht ohne Ihre Zustimmung installiert werden.

**Firewall**
Wählen Sie einen Filtermodus für die Firewall aus. Weitere Informationen finden Sie unter Filtermodi 20.

Nach der Installation von ESET Endpoint Security sollte der Computer auf Schadcode gescannt werden. Klicken Sie dazu im Hauptprogrammfenster auf **Computer scannen** und dann auf **Smart-Scan**. Weitere Informationen zum On-Demand-Scan finden Sie im Abschnitt On-Demand-Scan 14.

## 3.3 Remoteinstallation

Für eine Remoteinstallation können Sie ein Installationspaket erstellen, das über Remotedesktop-Software auf den gewünschten Rechnern installiert werden kann. Nach dem Abschluss der Installation können Sie ESET Endpoint Security mit ESET Remote Administrator remote verwalten.

Die Remoteinstallation gliedert sich in zwei Phasen:
1. Ein Remoteinstallationspaket über das ESET-Installationsprogramm erstellen 8
2. Remoteinstallation über Apple Remote Desktop 9

Mit der neuesten Version von ESET Remote Administrator 6 können Sie auch eine Remoteinstallation auf Clientcomputern mit OS X ausführen. Eine schrittweise Anleitung finden Sie in diesem Knowledgebase-Artikel. (Dieser Artikel ist möglicherweise nicht in Ihrer Sprache verfügbar.)

### 3.3.1 Ein Remoteinstallationspaket erstellen

**Programmkomponenten**
ESET Endpoint Security ermöglicht die Installation des Produkts ohne bestimmte Kernkomponenten (zum Beispiel ohne den Web- und E-Mail-Schutz). Deaktivieren Sie das Kontrollkästchen neben einer Produktkomponente, um sie aus der Installation zu entfernen.

**Proxyserver**
Wenn Sie einen Proxyserver verwenden, können Sie die entsprechenden Parameter festlegen, indem Sie die Option **Ich nutze einen Proxyserver** auswählen. Geben Sie im nächsten Fenster unter **Adresse** die IP-Adresse oder URL des Proxyservers ein. Geben Sie dann im Feld „Port“ den Port an, über den Verbindungen auf dem Proxyserver eingehen (standardmäßig 3128). Falls für den Proxyserver eine Authentifizierung erforderlich ist, geben Sie einen gültigen **Benutzernamen** und das **Passwort** ein. Wenn Sie keinen Proxyserver verwenden, wählen Sie die Option **Keinen Proxyserver verwenden**. Wenn Sie unsicher sind, ob Sie einen Proxyserver verwenden, können Sie Ihre aktuellen Systemeinstellungen verwenden. Wählen Sie dazu **Systemeinstellungen verwenden (empfohlen)**.

**Berechtigungen**
Im nächsten Schritt können Sie privilegierte Benutzer oder Gruppen definieren, die berechtigt sind, die Programmkonfiguration zu ändern. Wählen Sie links aus der Benutzerliste die Benutzer aus und fügen Sie sie über die Schaltfläche **Hinzufügen** zur Liste **Privilegierte Benutzer** hinzu. Um alle Systembenutzer anzuzeigen, wählen Sie die Option **Alle Benutzer anzeigen** aus. Wenn Sie die Liste der privilegierten Benutzer leer lassen, werden alle Benutzer als privilegiert betrachtet.

**ESET Live Grid**
Durch das ESET Live Grid-Frühwarnsystem ist ESET beim Auftauchen neuer Infiltrationen immer auf dem neuesten Stand und kann seine Kunden schneller schützen. Das System ermöglicht das Übermitteln von Informationen zu neuen Bedrohungen an das ESET-Virenlabor. Hier werden die Bedrohungen analysiert, verarbeitet und zur Signaturdatenbank hinzugefügt. Klicken Sie auf **Einstellungen**, um Einstellungen für das Einsenden verdächtiger Dateien festzulegen. Weitere Informationen finden Sie im Abschnitt Live Grid 27.

**Eventuell unerwünschte Anwendungen**
Im nächsten Schritt der Installation wird die Prüfung auf **Eventuell unerwünschte Anwendungen** konfiguriert. Bei eventuell unerwünschten Anwendungen handelt es sich um Programme, die zwar nicht unbedingt Sicherheitsrisiken in sich bergen, jedoch negative Auswirkungen auf das Verhalten Ihres Computers haben können. Diese Anwendungen sind oft mit anderen Programmen gebündelt und daher während des Installationsvorgangs schwer erkennbar. Obwohl bei solchen Anwendungen während der Installation gewöhnlich eine Benachrichtigung angezeigt wird, können sie auch leicht ohne Ihre Zustimmung installiert werden.

**Firewall**
Wählen Sie einen Filtermodus für die Personal Firewall aus. Weitere Informationen finden Sie unter Filtermodi 20.

**Dateien für Remoteinstallation**
Wählen Sie im letzten Schritt des Installationsassistenten einen Zielordner für das Installationspaket *(esets_remote_Install.pkg)*, das Shell-Skript für das Setup *(esets_setup.sh)* und das Shell-Skript für die Deinstallation *(esets_remote_UnInstall.sh)* aus.

### 3.3.2 Remoteinstallation auf den Zielrechnern

Zur Installation von ESET Endpoint Security auf den Zielrechnern können Sie Apple Remote Desktop oder ein anderes Tool verwenden, das normale Mac-Pakete (*.pkg*-Format) installieren, die Dateien kopieren und Shell-Skripte auf den Zielrechnern ausführen kann.

Um ESET Endpoint Security mit Apple Remote Desktop zu installieren, gehen Sie wie folgt vor:

1. Klicken Sie in Apple Remote Desktop auf das Symbol **Kopieren**.
2. Klicken Sie auf **+**, navigieren Sie zum Installations-Skript *(esets_setup.sh)* und wählen Sie es aus.
3. Wählen Sie **/tmp** aus dem Dropdownmenü **Objekte platzieren in** und klicken Sie auf **Kopieren**.
4. Klicken Sie auf **Installieren**, um das Paket an Ihren Zielcomputer zu senden.

Eine ausführliche Anleitung zur Administration der Clientcomputer mit ESET Remote Administrator finden Sie in der ESET Remote Administrator-Onlinedokumentation.

### 3.3.3 Remote-Deinstallation

Um ESET Endpoint Security von Clientrechnern zu deinstallieren, gehen Sie wie folgt vor:

1. Kopieren Sie mit dem Befehl **Elemente kopieren** von Apple Remote Desktop das Deinstallations-Skript (*esets_remote_unInstall.sh* – wird zusammen mit dem Installationspaket erstellt) in das /tmp-Verzeichnis der Zielrechner (z. B. */tmp/esets_remote_uninstall.sh*).
2. Wählen Sie unter **Befehl ausführen als** die Option **Benutzer** aus und geben Sie **root** im Feld **Benutzer** ein.
3. Klicken Sie auf **Senden**. Nach der erfolgreichen Deinstallation wird ein entsprechendes Konsolenprotokoll angezeigt.

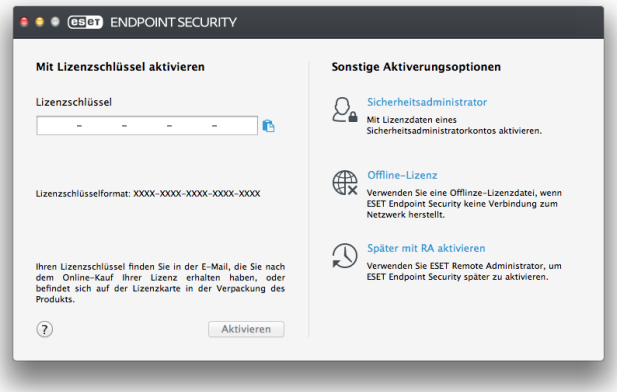
### 3.3.4 Remote-Upgrade

Über den Befehl **Pakete installieren** in Apple Remote Desktop können Sie jeweils die neueste Version von ESET Endpoint Security installieren, wenn eine neue Version veröffentlicht wird.

## 4. Produktaktivierung

Nach Abschluss der Installation werden Sie aufgefordert, Ihr Produkt zu aktivieren. Es stehen mehrere Aktivierungsmethoden zur Verfügung. Die Verfügbarkeit einer bestimmten Aktivierungsmethode hängt vom Land und von der Vertriebsart (CD/DVD, ESET-Webseite usw.) ab.

Um Ihr Exemplar von ESET Endpoint Security direkt aus der Anwendung zu aktivieren, klicken Sie auf das ESET Endpoint Security-Symbol in der OS X-Menüleiste (oben am Bildschirm) und dann auf **Produktaktivierung**. Sie können das Produkt auch im Hauptmenü unter **Hilfe** > **Lizenz verwalten** oder **Schutzstatus** > **Produkt aktivieren** aktivieren.


ENDPOINT SECURITY
Mit Lizenzschlüssel aktivieren
Lizenzschlüssel
Lizenzschlüsselformat: XXXX-XXXX-XXXX-XXXX-XXXX
Ihren Lizenzschlüssel finden Sie in der E-Mail, die Sie nach dem Online-Kauf Ihrer Lizenz erhalten haben, oder befindet sich auf der Lizenzkarte in der Verpackung des Produkts.
Aktivieren
Sonstige Aktivierungsoptionen
Sicherheitsadministrator
Mit Lizenzdaten eines Sicherheitsadministratorkontos aktivieren.
Offline-Lizenz
Verwenden Sie eine Offlinze-Lizenzdatei, wenn ESET Endpoint Security keine Verbindung zum Netzwerk herstellt.
Später mit RA aktivieren
Verwenden Sie ESET Remote Administrator, um ESET Endpoint Security später zu aktivieren.

Sie können ESET Endpoint Security mit einer der folgenden Methoden aktivieren:

- **Mit Lizenzschlüssel aktivieren** - Der Lizenzschlüssel ist eine eindeutige Zeichenkette im Format XXXX-XXXX-XXXX-XXXX-XXXX, die zur Identifizierung des Lizenzinhabers und zur Aktivierung der Lizenz verwendet wird. Sie finden den Lizenzschlüssel in der E-Mail, die Sie nach dem Kauf erhalten haben, oder auf der Lizenzkarte, die in der Produktverpackung enthalten ist.
- **Security Admin** - Ein im ESET Lizenzadministrator-Portal erstelltes Konto mit Anmeldedaten (E-Mail-Adresse und Passwort). Mit dieser Methode können Sie mehrere Lizenzen von einem Standort aus verwalten.
- **Offline-Lizenz** - Eine automatisch erzeugte Datei, die zum Zwecke der Bereitstellung von Lizenzinformationen in das ESET-Produkt übertragen wird. Die Offline-Lizenzdatei wird im ESET Lizenadministrator-Portal erzeugt und in Umgebungen verwendet, in denen die Anwendung keine Verbindung zur Lizenzierungsstelle herstellen kann.

Klicken Sie auf **Später mit RA aktivieren**, wenn der Computer Mitglied eines verwalteten Netzwerks ist und Ihr Administrator die Aktivierung mit ESET Remote Administrator ausführen möchte. Wählen Sie diese Option nur, wenn der Client später aktiviert werden soll.

**HINWEIS:** ESET Remote Administrator kann Clientcomputer mithilfe von Lizenzen, die der Administrator bereitstellt, im Hintergrund aktivieren.

# 5. Deinstallation

Das Deinstallationsprogramm für ESET Endpoint Security für Mac kann auf mehrere Arten gestartet werden:

- Legen Sie die Installations-CD/-DVD von ESET Endpoint Security in Ihren Computer ein, öffnen Sie sie über den Desktop oder ein **Finder**-Fenster und doppelklicken Sie auf **Deinstallieren**.
- Öffnen Sie die Installationsdatei von ESET Endpoint Security (*DMG*-Datei) und doppelklicken Sie auf **Deinstallieren**.
- Öffnen Sie im **Finder** den Ordner **Programme** auf Ihrer Festplatte, halten Sie die Ctrl-Taste gedrückt, klicken Sie auf das Symbol von **ESET Endpoint Security** und wählen Sie Option **Paketinhalt zeigen**. Öffnen Sie den Ordner **Contents** > **Helpers** und doppelklicken Sie auf das Symbol **Uninstaller**.

# 6. Übersicht

Das Hauptprogrammfenster von ESET Endpoint Security ist in zwei Abschnitte unterteilt. Das primäre Fenster (rechts) zeigt Informationen zu den im Hauptmenü (links) ausgewählten Optionen an.

Das Hauptmenü bietet Zugriff auf folgende Bereiche:

- **Schutzstatus** - liefert Informationen zum Schutzstatus Ihres Computers sowie zur Firewall und zum Web- und E-Mail-Schutz.
- **Computer scannen** - In diesem Bereich können Sie den On-Demand-Scan 14 konfigurieren und starten.
- **Update** - Dieser Bereich zeigt Informationen zu Updates der Signaturdatenbank an.
- **Einstellungen** - In diesem Abschnitt können Sie die Sicherheitsstufe Ihres Computers anpassen.
- **Tools** - Zugriff auf Log-Dateien 24, Taskplaner 26, Quarantäne 28, Ausgeführte Prozesse 30 und andere Programmfunktionen.
- **Hilfe** - Zugriff auf die Hilfedateien, die Internet-Knowledgebase, Supportanfrageformulare und zusätzliche Informationen zum Programm.

## 6.1 Tastaturbefehle

Folgende Tastaturbefehle können in Verbindung mit ESET Endpoint Security verwendet werden:

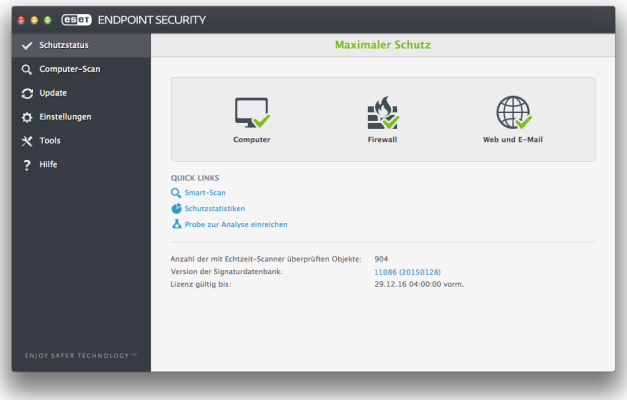
- *cmd+,* - zeigt ESET Endpoint Security-Einstellungen an.
- *cmd+O* - setzt das Hauptprogrammfenster von ESET Endpoint Security auf die Standardgröße zurück und positioniert es in der Bildschirmmitte.
- *cmd+Q* - blendet das ESET Endpoint Security Hauptprogrammfenster aus. Um es zu öffnen, klicken Sie auf das ESET Endpoint Security-Symbol in der OS X-Menüleiste (oben am Bildschirm).
- *cmd+W* - schließt das ESET Endpoint Security Hauptprogrammfenster.

Die folgenden Tastaturbefehle arbeiten nur, wenn die Option **Standardmenü verwenden** unter **Einstellungen** > **Erweiterte Einstellungen ...** > **Schnittstelle** aktiviert ist:

- *cmd+alt+L* - öffnet das Fenster **Log-Dateien**.
- *cmd+alt+S* - öffnet das Fenster **Taskplaner**.
- *cmd+alt+Q* - öffnet das Fenster **Quarantäne**.

### 6.2 Überprüfen der Funktionsfähigkeit des Systems

Um den Schutzstatus anzuzeigen, klicken Sie im Hauptmenü auf **Schutzstatus**. Im primären Fenster wird eine Darstellung des aktuellen Betriebszustands von ESET Endpoint Security angezeigt.




### 6.3 Vorgehensweise bei fehlerhafter Ausführung des Programms

Bei ordnungsgemäßer Funktion eines Moduls wird ein grünes Häkchen angezeigt. Wenn ein Modul nicht ordnungsgemäß funktioniert, wird ein rotes Ausrufezeichen oder ein oranges Benachrichtigungssymbol angezeigt. Zusätzlich werden in diesem Fall im Hauptprogrammfenster weitere Informationen zu dem Modul und ein Lösungsvorschlag angezeigt. Um den Status einzelner Module zu ändern, klicken Sie auf den blauen Link unter dem jeweiligen Hinweis.

Wenn Sie ein Problem mit den vorgeschlagenen Lösungen nicht beseitigen können, können Sie in der ESET-Knowledgebase nach einer Lösung suchen oder sich an den ESET-Support wenden. Der Support widmet sich umgehend Ihrem Anliegen, um schnell eine Lösung für Ihr Problem mit ESET Endpoint Security zu finden.

## 7. Computerschutz

Die Computerkonfiguration finden Sie unter **Einstellungen** > **Computer**. Sie zeigt den Status des **Echtzeit-Dateischutzes** an. Um die einzelnen Module zu deaktivieren, ändern Sie den Status des gewünschten Moduls in **DEAKTIVIERT**. Beachten Sie, dass dies die Schutzstufe des Computers herabsetzen kann. Um detaillierte Einstellungen für jedes Modul vorzunehmen, klicken Sie auf **Einstellungen**.

### 7.1 Viren- und Spyware-Schutz

Der Virenschutz bewahrt das System vor Angriffen, indem er potenziell gefährliche Dateien verändert. Wird eine Bedrohung durch Schadcode erkannt, kann das Virenschutz-Modul den Code unschädlich machen, indem es die Ausführung des Codes blockiert und dann den Code entfernt bzw. die Datei löscht oder in die Quarantäne verschiebt.

#### 7.1.1 Allgemein

Im Bereich **Allgemein** (**Einstellungen** > **Erweiterte Einstellungen ...** > **Allgemein**) können Sie die Erkennung der folgenden Arten von Anwendungen aktivieren:

- **Eventuell unerwünschte Anwendungen** - Diese Anwendungen sind nicht unbedingt und absichtlich schädlich, können jedoch die Leistung Ihres Computers beeinträchtigen. Als Benutzer werden Sie normalerweise vor deren Installation zur Bestätigung aufgefordert. Nach erfolgter Installation ändert sich das Systemverhalten (im Vergleich zum Verhalten vor der Installation). Dazu zählen vor allem ungewollte Popup-Fenster, die Aktivierung und Ausführung versteckter Prozesse, die erhöhte Inanspruchnahme von Systemressourcen, Änderungen in Suchergebnissen sowie die Kommunikation von Anwendungen mit Remote-Servern.
- **Potenziell unsichere Anwendungen** - In diese Kategorie fallen legitime Programme seriöser Hersteller, die jedoch von Angreifern ausgenutzt werden können, wenn sie ohne Wissen des Benutzers installiert werden. Da hierzu auch Programme für die Fernsteuerung von Computern gehören, ist diese Option standardmäßig deaktiviert.
- **Verdächtige Anwendungen** - Hierunter fallen Anwendungen, die mit sogenannten „Packer“- oder „Protector“-Programmen komprimiert wurden. Diese Art von Programmen wird oft von Malware-Autoren ausgenützt, um einer Erkennung zu entgehen. Packer sind selbst-extrahierende Anwendungen, die zur Laufzeit mehrere Arten von Malware in ein einziges Paket verpacken. Die gängigsten Packer sind UPX, PE_Compact, PKLite und ASPack. Dieselbe Malware kann unter Umständen unterschiedlich erkannt werden, wenn für die Kompression ein anderer Packer verwendet wurde. Packer können außerdem die „Signaturen“ regelmäßig verändern, wodurch Malware schwieriger zu erkennen und zu entfernen ist.

Klicken Sie auf **Einstellungen**, um Ausschlussfilter für Dateisystem bzw. Web- und E-Mail 12 einzurichten.

#### 7.1.1.1 Ausschlussfilter

Im Bereich **Ausschlussfilter** können Sie festlegen, dass bestimmte Dateien/Ordner, Anwendungen oder IP/IPv6-Adressen von Scans ausgenommen werden.

Dateien und Ordner, die auf der Registerkarte **Dateisystem** aufgeführt sind, werden von allen Scans ausgeschlossen: Scan der Systemstartdateien, Echtzeit-Scan und On-Demand-Scan.

- **Pfad** – Pfad zu den auszuschließenden Dateien/Ordnern
- **Bedrohung** – Steht neben einer ausgeschlossenen Datei der Name einer Bedrohung, so gilt die Ausnahme nicht generell für die Datei, sondern nur für diese bestimmte Bedrohung. Wird die Datei später durch andere Schadsoftware infiziert, erkennt der Virenschutz dies.
- **+** - Erstellen eines neuen Ausschlusses. Geben Sie den Pfad zum Objekt ein (Platzhalter *und ?werden unterstützt) oder wählen Sie den Ordner bzw. die Datei in der Baumstruktur aus.
- **−** – Löschen der ausgewählten Einträge
- **Standard** – annuliert alle Ausschlüsse

Auf der Registerkarte **Web und E-Mail** können Sie bestimmte **Anwendungen** oder **IP/IPv6-Adressen** von der Protokollprüfung ausschließen.

### 7.1.2 Systemstart-Schutz

Beim Scan der Systemstartdateien werden Dateien beim Systemstart automatisch untersucht. Dieser Scan wird standardmäßig als geplanter Task nach der Anmeldung eines Benutzers oder nach einem erfolgreichen Update der Viren-Datenbank ausgeführt. Klicken Sie auf **Einstellungen**, um die Einstellungen der ThreatSense-Engine für den Scan beim Systemstart zu ändern. Weitere Informationen zur Einrichtung der ThreatSense-Engine finden Sie in diesem Abschnitt 15.

### 7.1.3 Echtzeit-Dateischutz

Der Echtzeit-Dateischutz überwacht alle Datenträger und löst beim Eintreten bestimmter Ereignisse einen Scan aus. Durch die Verwendung unterschiedlicher ThreatSense-Technologien (siehe ThreatSense-Einstellungen 15) kann der Echtzeit-Dateischutz für neu erstellte Dateien von dem für bestehende Dateien abweichen. Neu erstellte Dateien können genauer kontrolliert werden.

Der Echtzeit-Dateischutz wird standardmäßig beim Systemstart gestartet und fortlaufend ausgeführt. In besonderen Fällen (z. B. bei einem Konflikt mit einem anderen Echtzeit-Scanner) kann der Echtzeit-Dateischutz durch Klicken auf das ESET Endpoint Security-Symbol ⓔ in der oberen Menüleiste und Auswählen der Option **Echtzeit-Dateischutz deaktivieren** beendet werden. Der Echtzeit-Dateischutz lässt sich auch im Hauptfenster beenden. Klicken Sie dazu auf **Einstellungen** > **Computer** und setzen Sie die Option **Echtzeit-Dateischutz** auf **DEAKTIVIERT**.

Um die erweiterten Einstellungen für den Echtzeit-Dateischutz zu ändern, wechseln Sie zu **Einstellungen** > **Erweiterte Einstellungen ...** (oder drücken *cmd+,*) > **Echtzeit-Schutz** und klicken neben **Erweiterte Einstellungen ...** auf **Einstellungen** (siehe Erweiterte Einstellungen für Scans 12).

#### 7.1.3.1 Scannen bei (Scannen bei Ereignis)

Standardmäßig werden alle Dateien beim Öffnen, Erstellen und Ausführen gescannt. Wir empfehlen, die Standardeinstellungen beizubehalten. So bietet der Echtzeit-Dateischutz auf Ihrem Computer maximale Sicherheit.

#### 7.1.3.2 Erweiterte Optionen für Scans

In diesem Fenster können Sie die von der ThreatSense -Engine zu scannenden Objekttypen festlegen, die **Advanced Heuristik** aktivieren bzw. deaktivieren sowie die Einstellungen für Archive und den Datei-Cache ändern.

Die Standardwerte im Abschnitt **Standard-Archiveinstellungen** sollten Sie nur ändern, um konkrete Probleme zu lösen, da höhere Archivverschachtelungswerte die Systemleistung beeinträchtigen können.

Sie können die Advanced Heuristik von ThreatSense für ausführbare, erstellte und geänderte Dateien einzeln ein- bzw. ausschalten. Aktivieren Sie dazu jeweils das Kontrollkästchen **Advanced Heuristik** im Abschnitt des entsprechenden ThreatSense-Parameters.

Um eine möglichst geringe Systembelastung während des Echtzeit-Dateischutzes zu gewährleisten, können Sie die Größe des Optimierungs-Cache festlegen. Der Optimierungs-Cache wird verwendet, wenn **Cache für nicht infizierte Dateien aktivieren** aktiviert ist. Ist diese Option deaktiviert, werden alle Dateien bei jedem Zugriff gescannt. Ansonsten werden nicht infizierte Dateien bis zur festgelegten Cache-Größe im Cache gespeichert und anschließend nicht mehr gescannt, es sei denn, sie wurden geändert. Nach einem Update der Signaturdatenbank werden die Dateien sofort wieder gescannt.

Klicken Sie auf **Cache für nicht infizierte Dateien aktivieren**, um diese Funktion zu aktivieren bzw. deaktivieren. Um die Größe des Cache festzulegen, geben Sie in das Eingabefeld neben **Cache-Größe** den gewünschten Wert ein.

Zusätzliche Scanparameter können im Fenster **ThreatSense-Einstellungen** festgelegt werden. Sie können angeben, welche Typen von **Objekten** gescannt werden sollen, mit welchen **Optionen** und auf welcher **Säuberungsstufe**. Außerdem können Sie die **Erweiterungen** und **Grenzen** für Dateigrößen für den Echtzeit-Dateischutz definieren. Das Fenster mit den ThreatSense-Einstellungen erreichen Sie über **Einstellungen** neben **ThreatSense-Engine** in den erweiterten Einstellungen. Ausführliche Informationen zu den ThreatSense-Einstellungen finden Sie im Abschnitt Einstellungen für ThreatSense 15.

#### 7.1.3.3 Wann sollten die Einstellungen für den Echtzeit-Dateischutz geändert werden?

Der Echtzeit-Dateischutz ist die wichtigste Komponente für ein sicheres System. Änderungen an den Parametern des Echtzeit-Dateischutzes sind mit Bedacht vorzunehmen. Es wird empfohlen, nur in einzelnen Fällen die Parameter zu ändern. Dies kann beispielsweise erforderlich sein, wenn ein Konflikt mit einer bestimmten Anwendung oder des Echtzeit-Scans eines anderen Virenschutzprogramms vorliegt.

Bei der Installation von ESET Endpoint Security werden alle Einstellungen optimal eingerichtet, um dem Benutzer die größtmögliche Schutzstufe für das System zu bieten. Um die Standardeinstellungen wiederherzustellen, klicken Sie auf die Schaltfläche **Standard** unten links im Fenster **Echtzeit-Dateischutz** (**Einstellungen** > **Erweiterte Einstellungen ...** > **Echtzeit-Schutz**).

#### 7.1.3.4 Echtzeit-Dateischutz prüfen

Um sicherzustellen, dass der Echtzeit-Dateischutz aktiv ist und Viren erkennt, verwenden Sie die Testdatei eicar.com. Diese Testdatei ist eine harmlose Datei, die von allen Virenschutzprogrammen erkannt wird. Die Datei wurde vom EICAR-Institut (European Institute for Computer Antivirus Research) erstellt, um die Funktionalität von Virenschutzprogrammen zu testen.

Um den Status des Echtzeit-Dateischutzes ohne den ESET Remote Administrator zu überprüfen, stellen Sie eine Remoteverbindung zum Clientcomputer über **Terminal** her und verwenden Sie den folgenden Befehl:

```
/Applications/.esets/Contents/MacOS/esets_daemon --status
```

Der Status des Echtzeit-Scanners wird entweder als `RTPStatus=Enabled` oder als `RTPStatus=Disabled` angezeigt.

Die Ausgabe des Terminal-Bash enthält folgende Status:

- auf dem Clientcomputer installierte Version von ESET Endpoint Security
- Datum und Version der Signaturdatenbank
- Pfad zum Update-Server

**HINWEIS:** Die Terminal-Nutzung wird nur für fortgeschrittene Benutzer empfohlen.

#### 7.1.3.5 Vorgehensweise bei fehlerhaftem Echtzeit-Dateischutz

In diesem Kapitel werden mögliche Probleme mit dem Echtzeit-Dateischutz sowie Lösungsstrategien beschrieben.

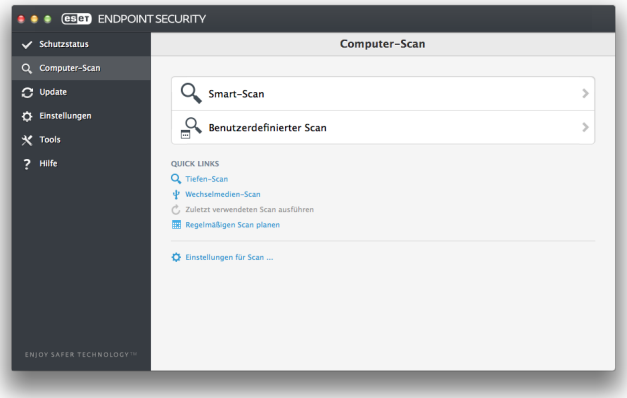
**Echtzeit-Dateischutz ist deaktiviert**
Der Echtzeit-Dateischutz wurde versehentlich von einem Benutzer deaktiviert und muss reaktiviert werden. Um den Echtzeit-Schutz erneut zu aktivieren, klicken Sie im Hauptmenü auf **Einstellungen** > **Computer** und setzen die Option **Echtzeit-Dateischutz** auf **AKTIVIERT**. Alternativ dazu können Sie den Echtzeit-Dateischutz in den erweiterten Einstellungen unter **Echtzeit-Schutz** aktivieren. Wählen Sie dazu **Echtzeit-Dateischutz aktivieren** aus.

**Echtzeit-Dateischutz erkennt und entfernt keinen Schadcode**
Stellen Sie sicher, dass keine anderen Virenschutzprogramme auf Ihrem Computer installiert sind. Zwei parallel ausgeführte Schutzprogramme können miteinander in Konflikt geraten. Wir empfehlen Ihnen, alle anderen Virusschutzprogramme zu deinstallieren.

**Echtzeit-Dateischutz startet nicht**
Wenn der Echtzeit-Dateischutz nicht automatisch beim Systemstart startet, können Konflikte mit anderen Programmen vorliegen. Wenden Sie sich in diesem Fall an den ESET-Support.

### 7.1.4 On-Demand-Scan

Wenn Sie den Verdacht haben, dass Ihr Computer infiziert ist (anormales Verhalten), führen Sie ein **Smart-Scan** aus, um Ihren Computer auf eingedrungene Schadsoftware zu untersuchen. Um maximalen Schutz zu gewährleisten, sollten Sie solche Scans routinemäßig durchführen und nicht nur, wenn eine Infektion vermutet wird. Durch regelmäßige Scans kann eingedrungene Schadsoftware erkannt werden, die vom Echtzeit-Dateischutz zum Zeitpunkt der Speicherung der Schadsoftware nicht erkannt wurde. Dies kommt z. B. vor, wenn der Echtzeit-Scan zum Zeitpunkt der Infektion deaktiviert war oder die Signaturdatenbank nicht auf dem neuesten Stand ist.




Sie sollten mindestens einmal im Monat einen On-Demand-Scan vornehmen. Sie können die Scans als Task unter **Tools** > **Taskplaner** konfigurieren.

Sie können auch ausgewählte Dateien und Ordner von Ihrem Desktop oder aus dem **Finder**-Fenster durch Ziehen und Ablegen auf dem Hauptbildschirm, Dock-Symbol, Menüleistensymbol (oberer Bildschirmrand) oder Anwendungssymbol (im Ordner */ Programme*) von ESET Endpoint Security ablegen.

#### 7.1.4.1 Scanmethode

Es gibt zwei verschiedene Arten von On-Demand-Scans. Beim **Smart-Scan** wird das System schnell gescannt, ohne dass Sie dafür weitere Scanparameter konfigurieren müssen. Bei der Methode **Benutzerdefinierter Scan** können Sie ein vordefiniertes Scanprofil und die zu scannenden Objekte auswählen.

##### 7.1.4.1.1 Smart-Scan

Mit dem Smart-Scan können Sie schnell den Computer scannen und infizierte Dateien säubern, ohne eingreifen zu müssen. Die Bedienung ist einfach, und es ist keine ausführliche Konfiguration erforderlich. Beim Smart-Scan werden alle Dateien in allen Ordnern gescannt, und erkannte eingedrungene Schadsoftware wird automatisch entfernt. Als Säuberungsstufe wird automatisch der Standardwert festgelegt. Weitere Informationen zu den Säuberungstypen finden Sie unter Säubern 16.

##### 7.1.4.1.2 Benutzerdefinierter Scan

Beim **Benutzerdefinierten Scan** können Sie verschiedene Scanparameter festlegen, z. B. die zu scannenden Objekte und die Scanmethoden. Der Vorteil dieser Methode ist die Möglichkeit zur genauen Parameterkonfiguration. Verschiedene Konfigurationen können als benutzerdefinierte Scanprofile gespeichert werden. Das ist sinnvoll, wenn Scans wiederholt mit denselben Parametern ausgeführt werden.

Zum Festlegen der zu scannenden Objekte wählen Sie **Computer scannen** > **Benutzerdefinierter Scan** und wählen dann bestimmte **Zu scannende Objekte** aus der Baumstruktur aus. Sie können ein zu scannendes Objekt auch genauer bestimmen, indem Sie den Pfad zu dem Ordner oder den Dateien eingeben, die gescannt werden sollen. Wenn Sie das System ohne zusätzliche Säuberung nur scannen möchten, wählen Sie die Option **Nur scannen, keine Aktion**. Außerdem können Sie zwischen drei Säuberungsstufen wählen. Klicken Sie dazu auf **Einstellungen** > **Säubern**.

**HINWEIS:** Ein Scan des Computers mit dieser Methode wird nur fortgeschrittenen Benutzern empfohlen, die Erfahrung im Umgang mit Virenschutzprogrammen haben.

#### 7.1.4.2 Zu scannende Objekte

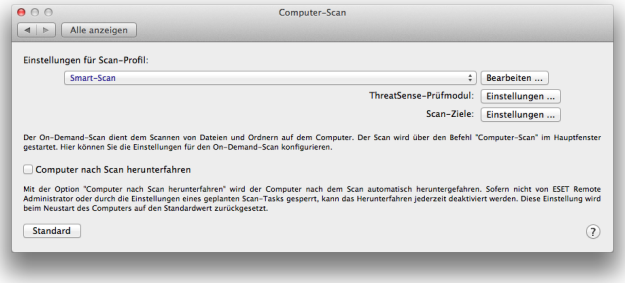
In der Baumstruktur der zu scannenden Objekte können Sie Dateien und Ordner auswählen, die auf Viren gescannt werden sollen. Je nach Profileinstellungen können Sie auch Ordner auswählen.

Sie können ein zu scannendes Objekt auch genauer definieren, indem Sie den Pfad zu dem Ordner oder den Dateien eingeben, die gescannt werden sollen. Wählen Sie die zu scannenden Objekte in der Baumstruktur der verfügbaren Ordner auf dem Computer aus, indem Sie das Kontrollkästchen neben einer Datei bzw. einem Ordner aktivieren.

#### 7.1.4.3 Scanprofile

Ihre benutzerdefinierten Einstellungen können für zukünftige Scans gespeichert werden. Wir empfehlen Ihnen, für jeden regelmäßig durchgeführten Scan ein eigenes Profil zu erstellen (mit verschiedenen zu scannenden Objekten, Scanmethoden und anderen Parametern).

Zur Erstellung eines neuen Profils klicken Sie im Hauptmenü auf **Einstellungen** > **Erweiterte Einstellungen ...** (oder drücken *cmd+,*) > **Computer scannen** und klicken auf **Bearbeiten** neben der Liste der aktuell bestehenden Profile.


Computer-Scan
Alle anzeigen
Einstellungen für Scan-Profil:
Smart-Scan
Bearbeiten ...
ThreatSense-Prüfmodul:
Einstellungen ...
Scan-Ziele:
Einstellungen ...
Der On-Demand-Scan dient dem Scannen von Dateien und Ordnern auf dem Computer. Der Scan wird über den Befehl "Computer-Scan" im Hauptfenster gestartet. Hier können Sie die Einstellungen für den On-Demand-Scan konfigurieren.
Computer nach Scan herunterfahren
Mit der Option "Computer nach Scan herunterfahren" wird der Computer nach dem Scan automatisch heruntergefahren. Sofern nicht von ESET Remote Administrator oder durch die Einstellungen eines geplanten Scan-Tasks gesperrt, kann das Herunterfahren jederzeit deaktiviert werden. Diese Einstellung wird beim Neustart des Computers auf den Standardwert zurückgesetzt.
Standard

Eine Beschreibung der einzelnen Scaneinstellungen finden Sie im Abschnitt Einstellungen für ThreatSense 15. So können Sie ein Scanprofil erstellen, das auf Ihre Anforderungen zugeschnitten ist.

Beispiel: Nehmen wir an, Sie möchten Ihr eigenes Scanprofil erstellen. Die Einstellungen des Smart-Scans eignen sich in gewissem Maße, aber Sie möchten nicht die laufzeitkomprimierten Dateien oder potenziell unsichere Anwendungen scannen. Außerdem möchten Sie die Option „Immer versuchen, automatisch zu säubern“ anwenden. Geben Sie im Fenster **Profile für On-Demand-Scanner** den Profilnamen ein, klicken Sie auf **Hinzufügen** und bestätigen Sie mit **OK**. Passen Sie dann die Einstellungen für **ThreatSense-Parameter** und **Zu scannende Objekte** an Ihre Anforderungen an.

Wenn Sie das Betriebssystem nach dem On-Demand-Scan abschalten und den Computer herunterfahren möchten, aktivieren Sie die Option **Computer nach Scan herunterfahren**.

### 7.1.5 Einstellungen für ThreatSense

ThreatSense ist eine proprietäre Technologie von ESET und besteht aus einer Kombination hochentwickelter Bedrohungserkennungsmethoden. Die Technologie arbeitet proaktiv, d. h. sie schützt das System auch während der ersten Stunden eines neuen Angriffs. Eingesetzt wird eine Kombination verschiedener Methoden (Code-Analyse, Code-Emulation, allgemeine Signaturen, Virussignaturen), die zusammen die Systemsicherheit deutlich erhöhen. Das Scanmodul kann verschiedene Datenströme gleichzeitig kontrollieren und so die Effizienz und Erkennungsrate steigern. ThreatSense entfernt erfolgreich Rootkits.

In den Einstellungen für ThreatSense können Sie verschiedene Scanparameter festlegen:

- Dateitypen und -erweiterungen, die gescannt werden sollen
- Die Kombination verschiedener Erkennungsmethoden
- Säuberungsstufen usw.

Um die Parameter des ThreatSense-Moduls für die verschiedenen Produktkomponenten zu konfigurieren, klicken Sie auf **Einstellungen > Erweiterte Einstellungen** und dann je nach gewünschter Komponente auf **Systemstart-Schutz**, **Echtzeit-Dateischutz** oder **Scannen des Computers** Klicken Sie neben dem ThreatSense-Modul auf „Einstellungen“, um für das gegebene Produktmodul Konfigurationsänderungen vorzunehmen. Die ThreatSense-Konfigurationseinstellungen sind auf fünf Registerkarten verteilt, wo Sie zu scannende Objekte, Scanmethoden, Säuberungseinstellungen, auszuschließende Dateierweiterungen, die maximale Dateigröße für zu scannende Dateien und die Verwendung der Smart-Optimierung konfigurieren können. Die nachfolgenden Abschnitte enthalten eine Beschreibung der Einstellungen auf diesen Registerkarten. Klicken Sie nach dem Vornehmen der Änderungen auf „OK“, um die Einstellungen für die ausgewählte Produktkomponente zu übernehmen.

- **Systemstart-Schutz** - Automatische Prüfung der Systemstartdateien
- **Echtzeit-Schutz** - Echtzeit-Dateischutz
- **Computer scannen** - On-Demand-Scan

Die ThreatSense-Parameter sind für jedes Modul optimal eingerichtet, und eine Veränderung der Einstellungen kann den Systembetrieb deutlich beeinflussen. So kann zum Beispiel eine Änderung der Einstellungen für das Scannen laufzeitkomprimierter Dateien oder die Aktivierung der Advanced Heuristik im Echtzeit-Dateischutz dazu führen, dass das System langsamer arbeitet. Es wird daher empfohlen, die Standard-Parameter für ThreatSense in allen Modulen unverändert beizubehalten. Änderungen sollten nur im Modul „Computer scannen“ vorgenommen werden.

#### 7.1.5.1 Objekte

Im Bereich **Objekte** können Sie festlegen, welche Dateien auf Infiltrationen gescannt werden sollen.

- **Symbolische Links** - (Nur beim Computerscan) Scan von Dateien, die eine Textfolge enthalten, die vom Betriebssystem als Pfad zu einer anderen Datei oder einem anderen Verzeichnis interpretiert wird.
- **E-Mail-Dateien** - (nicht verfügbar in Echtzeit-Dateischutz) Scan von E-Mail-Dateien.
- **Postfächer** – (nicht verfügbar in Echtzeit-Dateischutz) Scan von Benutzerpostfächern im System. Die unsachgemäße Anwendung dieser Option kann zu Konflikten mit Ihrem E-Mail-Programm führen. Weitere Informationen über Vor- und Nachteile dieser Option finden Sie im folgenden Knowledgebase-Artikel.
- **Archive** - (nicht verfügbar in Echtzeit-Dateischutz) Scan komprimierter Archivdateien (.rar, .zip, .arj, .tar usw.).
- **Selbstentpackende Archive** – (nicht verfügbar in Echtzeit-Dateischutz) Scan von Dateien in selbstentpackenden Archiven.
- **Laufzeitkomprimierte Dateien** - Laufzeitkomprimierte Dateien werden (anders als Standard-Archivtypen) im Arbeitsspeicher dekomprimiert. Wenn diese Option ausgewählt ist, werden statisch laufzeitkomprimierte Dateien (UPX, yoda, ASPack, FGS etc.) ebenfalls gescannt.

#### 7.1.5.2 Optionen

Im Bereich **Optionen** können Sie die Methoden festlegen, die bei einem Scan des Systems auf Infiltrationen angewendet werden sollen. Folgende Optionen stehen zur Verfügung:

- **Heuristik** – Heuristische Methoden verwenden einen Algorithmus, der (bösartige) Aktivitäten von Programmen analysiert. Mit ihrer Hilfe können bis dato unbekannte Schadprogramme oder Viren, die nicht in der Liste bekannter Viren (Signaturdatenbank) aufgeführt waren, erkannt werden.
- **Advanced Heuristik** – Als Advanced Heuristik werden besondere, von ESET entwickelte heuristische Verfahren bezeichnet, die für die Erkennung von Würmern und Trojanern optimiert sind, die in höheren Programmiersprachen geschrieben wurden. Advanced Heuristik ermöglicht eine wesentlich höhere Erkennungsrate des Programms.

#### 7.1.5.3 Säubern

In den Säuberungseinstellungen wird festgelegt, wie der Scanner die infizierten Dateien säubert. Es gibt drei Arten der Schadcodeentfernung:

- **Nicht säubern** - Der in infizierten Objekten erkannte Schadcode wird nicht automatisch entfernt. Eine Warnung wird angezeigt, und Sie werden aufgefordert, eine Aktion auszuwählen.
- **Normales Säubern** - Das Programm versucht, den Schadcode automatisch aus der Datei zu entfernen oder eine infizierte Datei zu löschen. Wenn es nicht möglich ist, die passende Aktion automatisch zu bestimmen, wird der Benutzer aufgefordert, eine Aktion auszuwählen. Diese Auswahl wird dem Benutzer auch dann angezeigt, wenn eine vordefinierte Aktion nicht erfolgreich abgeschlossen werden konnte.
- **Automatisch säubern** - Das Programm entfernt den Schadcode aus infizierten Dateien oder löscht diese Dateien (einschließlich Archiven). Ausnahmen gelten nur für Systemdateien. Wenn eine Datei nicht gesäubert werden kann, erhalten Sie eine Benachrichtigung und werden aufgefordert, die auszuführende Aktion auszuwählen.

***Warnung:*** Im Standardmodus „Normales Säubern“ wird das gesamte Archiv nur gelöscht, wenn es ausschließlich infizierte Dateien enthält. Wenn ein Archiv saubere und infizierte Dateien enthält, wird es nicht gelöscht. Im Modus „Automatisch säubern“ wird die gesamte Archivdatei gelöscht, auch wenn sie nicht infizierte Dateien enthält.

#### 7.1.5.4 Ausschlussfilter

Die Erweiterung ist der Teil eines Dateinamens nach dem Punkt. Erweiterungen definieren den Typ und den Inhalt der Datei. In diesem Teil der ThreatSense-Einstellungen können Sie die Dateitypen festlegen, die nicht gescannt werden sollen.

In der Standardeinstellung werden alle Dateien unabhängig von ihrer Erweiterung gescannt. Jede Erweiterung kann der Liste auszuschließender Dateien hinzugefügt werden. Über die Schaltflächen + und − können Sie festlegen, welche Erweiterungen gescannt werden sollen.

Der Ausschluss bestimmter Dateien ist dann sinnvoll, wenn das Scannen bestimmter Dateitypen die Funktion eines Programms beeinträchtigt. Beispielsweise kann es sinnvoll sein, Dateien mit der Erweiterung *log*, *cfg* oder *tmp* vom Scannen auszuschließen. Das richtige Format für die Angabe von Dateierweiterungen ist:
*log*
*cfg*
*tmp*

#### 7.1.5.5 Grenzen

Im Bereich **Grenzen** können Sie die Maximalgröße von Elementen und Stufen verschachtelter Archive festlegen, die gescannt werden sollen:

- **Maximale Größe:**Definiert die maximale Größe von zu scannenden Objekten. Der Virenschutz scannt dann nur die Elemente, deren Größe unter der angegebenen Maximalgröße liegt. Der Standardwert sollte nicht geändert werden; für gewöhnlich besteht dazu auch kein Grund. Diese Option sollte nur von fortgeschrittenen Benutzern geändert werden, die bestimmte Gründe dafür haben, größere Objekte vom Scan auszuschließen.
- **Maximale Scanzeit:**Definiert die maximale Dauer, die für das Scannen eines Objekts zur Verfügung steht. Wenn hier ein benutzerdefinierter Wert eingegeben wurde, beendet der Virenschutz das Scannen eines Elements, sobald diese Zeit abgelaufen ist, und zwar ungeachtet dessen, ob der Scan abgeschlossen ist oder nicht.
- **Maximale Verschachtelungstiefe:** Legt die maximale Tiefe des Archivscans fest. Der Standardwert 10 sollte nicht geändert werden; unter normalen Umständen besteht dazu auch kein Grund. Wenn der Scan aufgrund der Anzahl verschachtelter Archive vorzeitig beendet wird, bleibt das Archiv ungeprüft.
- **Maximale Dateigröße:** Über diese Option können Sie die maximale Dateigröße der entpackten Dateien festlegen, die in zu scannenden Archiven enthalten sind. Wenn der Scan aufgrund dieses Grenzwerts vorzeitig beendet wird, bleibt das Archiv ungeprüft.

#### 7.1.5.6 Weitere

**Smart-Optimierung aktivieren**
Die Smart-Optimierung passt die Einstellungen so an, dass ein wirksames Scannen bei gleichzeitig hoher Scangeschwindigkeit gewährleistet ist. Die verschiedenen Schutzmodule scannen auf intelligente Weise unter Einsatz verschiedener Scanmethoden. Die Smart-Optimierung ist innerhalb des Produkts nicht starr definiert. Das ESET-Entwicklungsteam fügt ständig neue Ergänzungen hinzu, die dann über die regelmäßigen Updates in Ihr ESET Endpoint Security integriert werden. Wenn die Smart-Optimierung deaktiviert ist, werden nur die benutzerdefinierten Einstellungen im ThreatSense-Kern des entsprechenden Moduls für das Scannen verwendet.

**AlternativenDatenstrom scannen** (nur On-Demand-Scanner)
Bei den von Dateisystemen verwendeten alternativen Datenströmen (Ressourcen-/Daten-Forks) handelt es sich um Datei- und Ordnerzuordnungen, die mit herkömmlichen Scantechniken nicht erkannt werden können. Eingedrungene Schadsoftware tarnt sich häufig als alternativer Datenstrom, um nicht erkannt zu werden.

### 7.1.6 Eingedrungene Schadsoftware wurde erkannt

Schadsoftware kann auf vielen Wegen in das System gelangen. Mögliche Infektionswege sind Webseiten, freigegebene Ordner, E-Mails oder Wechselmedien (USB-Sticks, externe Festplatten, CDs, DVDs usw.).

Wenn Ihr Computer die Symptome einer Malware-Infektion aufweist (Computer arbeitet langsamer als gewöhnlich, hängt sich oft auf usw.), sollten Sie folgendermaßen vorgehen:

1. Klicken Sie auf **Computer scannen**.
2. Klicken Sie auf **Smart-Scan** (weitere Informationen siehe Abschnitt Smart-Scan 14).
3. Nachdem der Scan abgeschlossen ist, überprüfen Sie im Log die Anzahl der gescannten, infizierten und gesäuberten Dateien.

Wenn Sie nur einen Teil Ihrer Festplatte scannen möchten, wählen Sie **Benutzerdefinierter Scan** und anschließend die Bereiche, die auf Viren gescannt werden sollen.

Das folgende allgemeine Beispiel zeigt, wie ESET Endpoint Security mit Schadsoftware umgeht. Angenommen, der Echtzeit-Dateischutz verwendet die Standard-Säuberungsstufe und erkennt eine eingedrungene Schadsoftware. Der Echtzeit-Dateischutz wird versuchen, den Schadcode aus der Datei zu entfernen oder die Datei zu löschen. Ist für den Echtzeitschutz keine vordefinierte Aktion angegeben, werden Sie in einem Warnfenster zur Auswahl einer Option aufgefordert. In der Regel stehen die Optionen **Säubern**, **Löschen** und **Keine Aktion** zur Auswahl. Es wird nicht empfohlen, die Option **Keine Aktion** zu wählen, da sonst die infizierte (n) Datei(en) nicht behandelt werden. Wählen Sie diese Option nur, wenn Sie sich sicher sind, dass die Datei harmlos ist und versehentlich erkannt wurde.

**Säubern und löschen** - Wählen Sie „Säubern“, wenn eine Datei von einem Virus mit Schadcode infiziert wurde. In einem solchen Fall sollten Sie zuerst versuchen, den Schadcode aus der infizierten Datei zu entfernen und ihren Originalzustand wiederherzustellen. Wenn die Datei ausschließlich Schadcode enthält, wird sie gelöscht.

**Dateien in Archiven löschen** - Im Standardmodus der Aktion „Säubern“ wird das gesamte Archiv nur gelöscht, wenn es ausschließlich infizierte Dateien enthält. Archive, die auch nicht infizierte Dateien enthalten, werden also nicht gelöscht. Die Option **Immer versuchen, automatisch zu säubern** sollten Sie mit Bedacht einsetzen, da in diesem Modus alle Archive gelöscht werden, die mindestens eine infizierte Datei enthalten, und zwar unabhängig vom Status der übrigen Archivdateien.

## 7.2 Web- und E-Mail-Schutz

Klicken Sie im Hauptmenü auf **Einstellungen** > **Web und E-Mail**, um auf den Web- und E-Mail-Schutz zuzugreifen. Sie können von dort aus auch auf ausführliche Einstellungen für die einzelnen Module zugreifen, indem Sie auf **Einstellungen** klicken.

**Web-Schutz** - Der Web-Schutz überwacht die HTTP/ HTTPS-Kommunikation zwischen Webbrowsern und Remoteservern.

**E-Mail-Schutz** - Der E-Mail-Schutz dient der Überwachung eingehender E-Mails, die mit dem POP3- oder IMAP-Protokoll übertragen werden.

**Phishing-Schutz** - Der Phishing-Schutz blockiert potenzielle Phishing-Angriffe von Websites oder Domänen, die in der Schadsoftware-Datenbank von ESET enthalten sind.

**Web-Kontrolle** - Sperrt Webseiten, die möglicherweise unerlaubte oder ungeeignete Inhalte enthalten.

### 7.2.1 Web-Schutz

Der Web-Schutz dient zur Überwachung von Verbindungen zwischen Webbrowsern und Remote-Servern auf die Einhaltung der Regeln des HTTP (Hypertext Transfer Protocol)- bzw. HTTPS-Protokolls.

#### 7.2.1.1 Ports

Auf der Registerkarte **Ports** können Sie die für HTTP-Verbindungen verwendeten Portnummern definieren. In der Standardeinstellung sind die Portnummern 80, 8080 und 3128 vorgegeben.

#### 7.2.1.2 Aktiver Modus

ESET Endpoint Security enthält außerdem das Untermenü **Aktiver Modus**, in dem der Prüfungsmodus für Webbrowser festgelegt wird. Im aktiven Modus werden Daten untersucht, die von Anwendungen mit Internetzugriff übertragen werden, unabhängig davon, ob diese Anwendungen Webbrowser sind. Ist der aktive Modus nicht aktiviert, wird die Kommunikation der Anwendungen nur Stück für Stück überwacht. Dies verringert die Effizienz der Datenverifizierung, erhöht jedoch die Kompatibilität mit den aufgeführten Anwendungen. Verursacht das Verfahren keine Probleme, sollten Sie den aktiven Modus einschalten, indem Sie das Kontrollkästchen der gewünschten Anwendung aktivieren.

Wenn eine überwachte Anwendung Daten herunterlädt, werden diese von ESET Endpoint Security zunächst in einer temporären Datei gespeichert, jedoch noch nicht an die betreffende Anwendung weitergegeben. Nach Abschluss des Downloads werden die Daten dann auf Schadcode überprüft. Wenn keine Infiltration gefunden wird, werden die Daten an die Anwendung übergeben. Auf diese Weise kann der Datenverkehr überwachter Anwendungen vollständig geprüft werden. Wenn hingegen der passive Modus aktiviert ist, werden die Daten stückweise an die betreffende Anwendung weitergegeben, um Fehler durch Zeitüberschreitung zu vermeiden.

#### 7.2.1.3 URL-Listen

Im Bereich **URL-Listen** können Sie HTTP-Adressen angeben, die gesperrt, zugelassen oder von der Prüfung ausgeschlossen werden sollen. Auf Websites in der Liste der gesperrten Adressen kann nicht zugegriffen werden. Auf Websites in der Liste der ausgeschlossenen Adressen kann zugegriffen werden, ohne dass diese auf Schadcode gescannt werden.

Um nur den Zugriff auf die in der Liste **Zugelassene URLs** enthaltenen URLs zu erlauben, wählen Sie **URL-Zugriff einschränken** aus.

Um eine Liste zu aktivieren, wählen Sie neben dem Listennamen die Option **Aktiviert** aus. Wenn Sie benachrichtigt werden möchten, wenn Sie eine Adresse aus der gegenwärtigen Liste eingeben, wählen Sie **Hinweis anzeigen** aus.

Die Sonderzeichen *(Sternchen) und ?(Fragezeichen) können beim Erstellen von URL-Listen als Platzhalter verwendet werden. Das Sternchen steht für eine beliebige Zeichenfolge, das Fragezeichen für ein beliebiges Zeichen. Die Liste der ausgeschlossenen Adressen sollten Sie mit Bedacht zusammenstellen. Geben Sie ausschließlich vertrauenswürdige und sichere Adressen an. Achten Sie außerdem darauf, dass die Zeichen „*“ und „?“ korrekt verwendet werden.

### 7.2.2 E-Mail-Schutz

Der E-Mail-Schutz dient der Überwachung eingehender E-Mails, die mit dem POP3- oder IMAP-Protokoll übertragen werden. Für die Prüfung eingehender Nachrichten verwendet das Programm alle erweiterten ThreatSense-Prüfmethoden. Die Erkennung von Schadcode findet also noch vor dem Abgleich mit der Signaturdatenbank statt. Das Scannen des POP3- und IMAP-Datenverkehrs erfolgt unabhängig vom verwendeten E-Mail-Programm.

**ThreatSense-Prüfmodul** - In den erweiterten Prüfeinstellungen können Sie die zu scannenden Objekte, die Erkennungsmethoden usw. konfigurieren. Klicken Sie auf **Einstellungen**, um die ausführlichen Scaneinstellungen anzuzeigen.

An jede E-Mail, die gescannt wurde, kann ein Prüfhinweis mit den Scanergebnissen angehängt werden. Hierzu können Sie die Option **Prüfhinweise zu E-Mail-Betreff hinzufügen** aktivieren. Auf diese Hinweise sollte sich der Empfänger jedoch nicht unbesehen verlassen, da sie bei problematischen HTML-Nachrichten eventuell verloren gehen oder von manchen Viren auch gefälscht werden können. Folgende Optionen stehen zur Verfügung:

**Nie** - Es werden keine Prüfhinweise hinzugefügt.
**Nur bei infizierten E-Mails** - Nur Nachrichten mit Schadsoftware werden als geprüft gekennzeichnet.
**Bei allen geprüften E-Mails** - Es werden Prüfhinweise an alle geprüften E-Mails angehängt.

**Text, der zur Betreffzeile infizierter E-Mails hinzugefügt wird** - Hier können Sie das Betreffpräfix für infizierte E-Mails bearbeiten.

**Prüfhinweise am Ende der E-Mail hinzufügen** - Aktivieren Sie dieses Kontrollkästchen, wenn zu infizierten E-Mails eine Virenwarnung hinzugefügt werden soll. Auf diese Weise können infizierte Nachrichten leicht gefiltert werden. Die Warnung erhöht außerdem die Glaubwürdigkeit beim Empfänger und bietet beim Erkennen einer Infiltration wertvolle Informationen zur Gefährdung durch eine bestimmte E-Mail oder einen Absender.

#### 7.2.2.1 Prüfen des POP3-Protokolls

Das POP3-Protokoll ist das am weitesten verbreitete Protokoll für den Empfang von E-Mails mit einer E-Mail-Client-Anwendung. ESET Endpoint Security bietet Schutz für dieses Protokoll unabhängig vom verwendeten E-Mail-Client.

Das Modul für diesen Schutz wird beim Systemstart automatisch gestartet und bleibt danach im Arbeitsspeicher aktiv. Vergewissern Sie sich, dass das Modul aktiviert ist, damit der Protokollfilter richtig funktioniert. Die Prüfung des POP3-Protokolls wird automatisch ausgeführt, ohne dass Sie den E-Mail-Client neu konfigurieren müssen. Standardmäßig wird der gesamte Datenverkehr über Port 110 geprüft; weitere Kommunikationsports können bei Bedarf hinzugefügt werden. Die Portnummern müssen mit einem Komma voneinander getrennt werden.

Wenn **Prüfen von E-Mails per POP3-Protokoll aktivieren** aktiviert ist, wird der gesamte über das POP3-Protokoll empfangene Verkehr auf Schadsoftware überwacht.

#### 7.2.2.2 Prüfen des IMAP-Protokolls

Das Internet Message Access Protocol (IMAP) ist ein weiteres Internetprotokoll für den Abruf von E-Mails. IMAP bietet gegenüber POP3 einige Vorteile. Beispielsweise können sich mehrere Clients gleichzeitig beim selben Postfach anmelden und Statusinformationen zu den Nachrichten pflegen, z. B. ob die Nachricht gelesen, beantwortet oder gelöscht wurde. ESET Endpoint Security schützt dieses Protokoll unabhängig vom eingesetzten E-Mail-Programm.

Das Modul für diesen Schutz wird beim Systemstart automatisch gestartet und bleibt danach im Arbeitsspeicher aktiv. Vergewissern Sie sich, dass die Prüfung des IMAP-Protokolls aktiviert ist, damit das Modul richtig funktioniert. Die Prüfung des IMAP-Protokolls wird automatisch ausgeführt, ohne dass Sie den E-Mail-Client neu konfigurieren müssen. Standardmäßig wird der gesamte Datenverkehr über Port 143 geprüft; weitere Kommunikationsports können bei Bedarf hinzugefügt werden. Die Portnummern müssen mit einem Komma voneinander getrennt werden.

Wenn **Prüfen von E-Mails per IMAP-Protokoll aktivieren** aktiviert ist, wird der gesamte über das IMAP-Protokoll empfangene Verkehr auf Schadsoftware überwacht.

### 7.3 Phishing-Schutz

Der Ausdruck *Phishing* bezeichnet kriminelle Vorgehensweisen unter Verwendung von Social-Engineering-Techniken (Manipulation von Anwendern, um an vertrauliche Daten zu gelangen). Phishing zielt darauf ab, an vertrauliche Daten wie Konto- und Kreditkartennummern, PIN-Codes, Benutzernamen oder Passwörter zu gelangen.

Wir empfehlen, den Phishing-Schutz aktiviert zu lassen (**Einstellungen** > **Erweiterte Einstellungen ...** > **Phishing-Schutz**). Alle potenziellen Phishing-Angriffe von Webseiten oder Domänen, die in der ESET-Malwaredatenbank aufgeführt sind, werden blockiert, und Sie erhalten einen Warnhinweis über den Angriffsversuch.

## 8. Firewall

Die Personal Firewall steuert den gesamten ein- und ausgehenden Netzwerkverkehr des Systems, indem sie einzelne Netzwerkverbindungen je nach den spezifierten Filterregeln zulässt oder verweigert. So bietet die Firewall Schutz gegen Angriffe von Remotecomputern und ermöglicht das Blockieren bestimmter Dienste. Darüber hinaus bietet sie einen Virenschutz für die Protokolle HTTP, POP3 und IMAP.

Die Konfiguration für die Personal Firewall finden Sie unter **Einstellungen** > **Firewall**. Dort können Sie den Filtermodus auswählen, Regeln festlegen und weitere Einstellungen vornehmen. Außerdem können Sie auf genauere Einstellungen des Programms zugreifen.

Wenn Sie die Option **Alle Netzwerkverbindungen blockieren: Netzwerk trennen** aktivieren, werden alle ein- und ausgehenden Verbindungen von der Personal Firewall blockiert. Verwenden Sie diese Option nur, wenn Sie schwerwiegende Sicherheitsrisiken befürchten, die eine Trennung der Netzwerkverbindung erfordern.

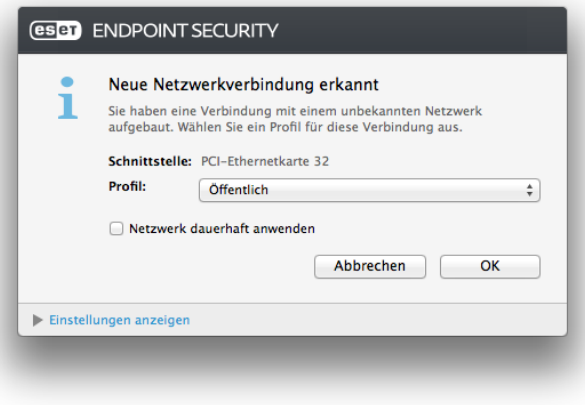
### 8.1 Filtermodi

Für die ESET Endpoint Security-Personal Firewall stehen drei Filtermodi zur Auswahl. Die Einstellungen für die Filtermodi finden Sie unter „Einstellungen“ > „Erweiterte Einstellungen“ > **Firewall**. Das Verhalten der Firewall ändert sich je nach gewähltem Modus. Der Filtermodus bestimmt auch, wie stark der Anwender eingreifen muss.

**Alle Verbindungen blockiert** - Sämtliche ein- und ausgehenden Verbindungen werden blockiert.

**Automatisch mit Ausnahmen** - Dies ist der Standardmodus. Dieser Modus eignet sich für Anwender, die eine möglichst einfache und praktische Nutzung der Firewall wünschen, bei der keine Regeln erstellt werden müssen. Im Automatikmodus ist der ausgehende Standarddatenverkehr für das System zugelassen und nicht initiierte Verbindungen aus dem Netzwerk werden blockiert. Sie haben auch die Möglichkeit, benutzerdefinierte Regeln hinzuzufügen.

**Interaktiv** - Mit diesem Modus können Sie eine benutzerdefinierte Konfiguration für Ihre Personal Firewall erstellen. Wenn eine Verbindung erkannt wird und keine Regel dafür existiert oder gilt, wird in einem Dialogfenster eine unbekannte Verbindung gemeldet. Der Benutzer kann entscheiden, ob die Verbindung zugelassen oder blockiert werden soll, und diese Auswahl kann als neue Regel für die Personal Firewall übernommen werden. Wenn eine neue Regel erstellt wurde, werden Verbindungen dieser Art beim nächsten Verbindungsversuch entsprechend der Regel automatisch zugelassen oder blockiert.




Um genaue Informationen zu allen blockierten Verbindungen in einer Log-Datei zu speichern, aktivieren Sie die Option **Alle blockierten Verbindungen in Log aufnehmen**. Um die Log-Dateien der Firewall zu prüfen, klicken Sie im Hauptmenü auf **Tools** > **Logs** und wählen Sie **Firewall** aus dem Dropdown-Menü **Log**.

## 8.2 Firewall-Regeln

Regeln fassen verschiedene Bedingungen zusammen, mit denen alle Netzwerkverbindungen getestet werden, und die Aktionen, die diesen Bedingungen zugewiesen sind. Über die Regeln der Personal Firewall können Sie festlegen, welche Art Aktion ausgeführt werden soll, wenn eine Verbindung aufgebaut wird, für die eine Regel existiert.

Eingehende Verbindungen stammen von Remotecomputern, die versuchen, eine Verbindung mit dem lokalen System aufzubauen. Ausgehende Verbindungen funktionieren umgekehrt - das lokale System nimmt Kontakt mit einem Remotecomputer auf.

Wenn eine neue unbekannte Verbindung erkannt wird, sollten Sie sich gut überlegen, ob Sie sie zulassen oder blockieren. Ungebetene, unsichere oder unbekannte Verbindungen stellen ein Sicherheitsrisiko für das System dar. Wenn eine solche Verbindung aufgebaut wurde, empfehlen wir Ihnen, genau auf den Remotecomputer und die Anwendung, die versucht, auf Ihren Computer zuzugreifen, zu achten. Viele Infiltrationen versuchen, an private Daten zu gelangen, solche Daten zu senden oder weitere Schadprogramme auf den Computer herunterzuladen. Mit der Personal Firewall können Sie solche Verbindungen erkennen und beenden.

### 8.2.1 Erstellen neuer Regeln

Die Registerkarte **Regeln** enthält eine Liste aller Regeln, die auf den Datenverkehr der einzelnen Anwendungen angewendet werden. Regeln werden automatisch gemäß der Reaktion des Anwenders bei einer neuen Verbindung hinzugefügt.

Klicken Sie auf **Hinzufügen ...**, um eine neue Regel zu erstellen. Geben Sie dann einen Namen für die Regel und fügen Sie das Anwendungssymbol durch Ziehen und Ablegen in das leere Feld ein oder klicken auf **Durchsuchen**, um die Anwendung im Ordner */ Programme* zu suchen. Wenn Sie die Regel auf alle Anwendungen anwenden möchten, die auf Ihrem Computer installiert sind, wählen Sie **Alle Anwendungen** aus.

Wählen Sie im nächsten Fenster die gewünschte **Aktion** (Kommunikation zwischen ausgewählter Anwendung und Netzwerk zulassen oder blockieren) und die **Richtung** des Datenverkehrs (eingehend, ausgehend oder beides). Wählen Sie **Regel in Log schreiben** aus, um die gesamte von dieser Regel betroffene Kommunikation aufzuzeichnen. Um die Firewall-Logs zu prüfen, klicken Sie im ESET Endpoint Security-Hauptmenü auf **Tools** > **Logs** und wählen Sie **Firewall** aus dem Dropdown-Menü **Log** aus.

Legen Sie im Bereich **Protokoll/Ports** das Protokoll und den Port fest, die von der Anwendung zur Kommunikation verwendet werden (wenn das TCP- oder UDP-Protokoll ausgewählt ist). Die Transportprotokoll-Ebene ermöglicht einen sicheren und effizienten Datentransfer.

Geben Sie zuletzt die Zielkriterien für die Regel (IP-

Adressen, Bereich, Teilnetz, Ethernet oder Internet) ein.

### 8.3 Firewall-Zonen

Eine Zone besteht aus einer Sammlung von Netzwerkadressen, die eine logische Gruppe ergeben. Jeder Adresse in einer Gruppe werden die gleichen Regeln zugewiesen, die zentral für die gesamte Gruppe erstellt werden.

Sie können solche Zonen erstellen, indem Sie auf die Schaltfläche **Hinzufügen** klicken. Geben Sie einen Namen im Feld **Name** und eine **Beschreibung** (optional) der Zone ein. Wählen Sie ein Profil aus, dem die Zone zugewiesen werden soll, und fügen Sie eine IPv4-/IPv6-Adresse, einen Adressbereich, ein Subnetz, ein WLAN-Netzwerk oder eine Schnittstelle hinzu.

### 8.4 Firewall-Profile

Über die Option **Profile** können Sie das Verhalten der Personal Firewall von ESET Endpoint Security steuern. Sie können Firewall-Regeln während der Erstellung oder Bearbeitung einem bestimmten Profil zuweisen. Wenn Sie ein Profil auswählen, werden nur die globalen Regeln (ohne ausgewähltes Profil) und die diesem Profil zugewiesenen Regeln angewendet. Sie können mehrere Profile mit unterschiedlichen Regeln erstellen, um das Verhalten der Personal Firewall schnell und einfach zu ändern.

### 8.5 Firewall-Logs

Die Personal Firewall von ESET Endpoint Security speichert alle wichtigen Ereignisse in einer Log-Datei. Um auf die Log-Dateien der Firewall zuzugreifen, klicken Sie im Hauptmenü auf **Tools** > **Logs** und wählen Sie **Firewall** aus dem Dropdown-Menü **Log** aus.

Die Log-Dateien sind ein wertvolles Instrument zum Erkennen von Fehlern und zum Aufdecken von versuchten Zugriffen auf das System. Die Log-Dateien der ESET-Personal Firewall enthalten folgende Daten:

- Datum und Uhrzeit des Ereignisses
- Name des Ereignisses
- Quelle
- Zielnetzwerkadresse
- Kommunikationsprotokoll
- Angewendete Regel oder ggf. Name des Wurms
- Betroffene Anwendung
- Benutzer

Eine gründliche Analyse dieser Daten kann zur Erkennung von Sicherheitsbedrohungen beitragen. Viele weitere Faktoren, die potenzielle Sicherheitsrisiken darstellen, können mit der Personal Firewall kontrolliert werden: häufige Verbindungen von unbekannten Standorten, ungewöhnlich viele Verbindungsversuche, Verbindungen mit unbekannten Anwendungen, ungewöhnliche Portnummern.

## 9. Medienkontrolle

Mit ESET Endpoint Security können Sie Medien bzw. Geräte scannen oder sperren oder erweiterte Filter- und/oder Berechtigungseinstellungen anpassen und definieren, wie ein Benutzer auf diese Geräte zugreifen und mit ihnen arbeiten kann. Dies ist sinnvoll, wenn der Administrator verhindern möchte, dass Benutzer Geräte mit unerwünschten Inhalten verwenden.

Unterstützte externe Geräte:
- Datenträgerspeicher (Festplatten, USB-Speicher)
- CD/DVD
- USB-Drucker
- Bildverarbeitungsgerät
- Serieller Port
- Netzwerk
- Mobiles Gerät

Wenn ein von einer bestehenden Regel blockiertes Gerät eingefügt wird, wird ein Benachrichtigungsfenster angezeigt und es wird kein Zugriff auf das Gerät gewährt.

Im Log der Medienkontrolle werden alle Ereignisse aufgezeichnet, die die Medienkontrolle auslösen. Um Log-Einträge anzuzeigen, klicken Sie im Hauptfenster von ESET Endpoint Security auf **Tools** > **Log-Dateien** 24.

### 9.1 Regel-Editor

Die Einstellungen der Medienkontrolle können unter **Einstellungen** > **Erweiterte Einstellungen ...** > **Medienkontrolle** geändert werden.

Durch Klicken auf **Medienkontrolle aktivieren** wird die Funktion der Medienkontrolle in ESET Endpoint Security aktiviert. Nach der Aktivierung der Medienkontrolle können Sie Regeln für die Medienkontrolle verwalten und bearbeiten. Über das Kontrollkästchen neben einem Regelnamen können Sie die entsprechende Regel aktivieren und deaktivieren.

Mit den Schaltflächen + und − können Sie Regeln hinzufügen und entfernen. Die Regeln sind nach absteigender Priorität geordnet (Regeln mit höchster Priorität werden an oberster Stelle angezeigt). Um die Reihenfolge zu ändern, bringen Sie die Regeln durch Ziehen und Ablegen in eine andere Position oder klicken Sie auf und wählen Sie eine der Optionen aus.

ESET Endpoint Security erkennt automatisch alle aktuell eingelegten Geräte und deren Parameter (Gerätetyp, Hersteller, Modell, Seriennummer). Statt Regeln manuell zu erstellen, können Sie auch auf **Auffüllen** klicken, das Gerät auswählen und durch Klicken auf **Weiter** die Regel erstellen.

Bestimmte Gerätetypen können je nach Benutzer oder Benutzergruppen oder auf Grundlage weiterer, in der Regelkonfiguration festgelegter Parameter zugelassen oder gesperrt werden. Die Liste der Regeln enthält verschiedene Angaben wie Regelname, Geräteart, Logging-Schweregrad und auszuführende Aktion beim Anschließen eines Geräts an den Computer.

**Name**

Geben Sie zur leichteren Identifizierung der Regel im Feld **Name** eine Beschreibung ein. Über das Kontrollkästchen neben **Regel aktiviert** wird die Regel deaktiviert bzw. aktiviert. Dies ist beispielsweise nützlich, wenn Sie eine Regel deaktivieren, jedoch nicht dauerhaft löschen möchten.

**Gerätetyp**

Wählen Sie im Dropdown-Menü den gewünschten Typ des externen Geräts aus. Gerätetypinformationen werden über das Betriebssystem erfasst. Speichergeräte umfassen externe Datenträger oder herkömmliche Kartenlesegeräte, die über den USB- oder FireWire-Anschluss an den Computer angeschlossen sind. Smartcard-Leser bezeichnen Geräte, die beliebige Medien mit einem eingebettetem integrierten Schaltkreis lesen, wie SIM-Karten oder Authentifizierungskarten. Bildverarbeitungsgeräte sind beispielsweise Scanner oder Kameras. Diese Geräte stellen nur Informationen zu den eigenen Aktionen bereit, keine Benutzerinformationen. Daher können diese Geräte nur global blockiert werden.

**Aktion**

Der Zugriff auf andere Geräte als Speichergeräte kann entweder zugelassen oder gesperrt werden. Im Gegensatz dazu ist es für Speichergeräte möglich, eines der folgenden Rechte für die Regel auszuwählen:
**Lese-/Schreibzugriff** - Der vollständige Zugriff auf das Gerät wird zugelassen.
**Nur Lesezugriff** - Nur Lesezugriff auf das Gerät wird zugelassen.
**Sperren** - Der Zugriff auf das Gerät wird gesperrt.

**Kriterientyp**

Wählen Sie **Gerätegruppe** oder **Gerät** aus. Nachfolgend sind weitere Parameter zur Feinanpassung der Regeln und Anpassung an bestimmte Geräte aufgeführt.
**Hersteller** - Ermöglicht das Filtern der Liste nach Herstellername oder -ID.
**Modell** - Die Bezeichnung des Geräts.
**Seriennummer** - Externe Geräte verfügen üblicherweise über eigene Seriennummern. Bei CDs/DVDs bezieht sich die Seriennummer auf das Exemplar, nicht auf das CD/DVD-Laufwerk.

**HINWEIS:** Wenn diese Parameter nicht definiert werden, ignoriert die Regel diese Felder bei der Abstimmung. Bei Filterparametern mit Textfeldern muss die Groß-/Kleinschreibung nicht beachtet zu werden. Platzhalter (*, ?) werden nicht unterstützt.

**TIPP:** Um Informationen zu einem Gerät anzuzeigen, können Sie eine Regel für die entsprechende Geräteart erstellen und das Gerät an den Computer anschließen. Nachdem das Gerät angeschlossen wurde, werden die Gerätedetails im Medienkontrolle-Log 24 angezeigt.

**Logging-Schweregrad**

**Immer** - Alle Ereignisse werden protokolliert.
**Diagnose** - Informationen, die für die Feineinstellung des Programms benötigt werden, werden protokolliert.
**Informationen** - Zeichnet zusätzlich zu den oben genannten Einträgen informative Meldungen auf.
**Warnungen** - Kritische Fehler und Warnungen werden protokolliert.
**Keine** - Es werden keine Logs aufgezeichnet.

**Benutzerliste**

Die Regeln können auf bestimmte Benutzer oder Benutzergruppen beschränkt werden, indem Sie diese zur Benutzerliste hinzufügen:
**Bearbeiten ...** – Öffnet den **Identitäts-Editor**, in dem Sie Benutzer oder Gruppen auswählen können. Um eine Liste von Benutzern einzurichten, wählen Sie die gewünschten Benutzer links in der Liste **Benutzer** aus und klicken auf **Hinzufügen**. Um einen Benutzer zu entfernen, wählen Sie ihn in der Liste **Ausgewählte Benutzer** aus und klicken auf **Entfernen**. Um alle Systembenutzer anzuzeigen, wählen Sie die Option **Alle Benutzer anzeigen** aus. Wenn diese Liste leer ist, werden alle Benutzer zugelassen.

**HINWEIS:** Nicht alle Geräte können über Benutzerregeln eingeschränkt werden (Bildverarbeitungsgeräte liefern beispielsweise keine Informationen über Benutzer, sondern nur über ausgeführte Aktionen).

## 10. Web-Kontrolle

Mit der Funktion **Web-Kontrolle** können Sie Einstellungen konfigurieren, die dazu beitragen, Ihr Unternehmen vor Situationen zu schützen, für die es gesetzlich haftet. So kann mit der Web-Kontrolle beispielsweise der Zugriff auf Websites geregelt werden, die Urheberrechte verletzen. Ziel ist es, Mitarbeiter am Zugriff auf Webseiten mit ungeeigneten oder schädlichen Inhalten bzw. mit negativem Einfluss auf die Produktivität zu hindern. Arbeitgeber oder Systemadministratoren können mit dieser Funktion den Zugriff auf über 27 vordefinierte Webseitenkategorien und über 140 Unterkategorien unterbinden.

Die Web-Kontrolle ist standardmäßig deaktiviert. Um sie zu aktivieren, klicken Sie auf **Einstellungen** > **Erweiterte Einstellungen** > **Web-Kontrolle** und aktivieren Sie das Kontrollkästchen neben **Web-Kontrolle aktivieren**.

Im Fenster „Regel-Editor“ werden vorhandene URL-basierte oder Kategorie-basierte Regeln angezeigt. Die Liste der Regeln enthält verschiedene Angaben zu jeder Regel, wie Regelname, Art des Sperrens, auszuführende Aktion nach dem Zuordnen einer Regel der Web-Kontrolle und Log 24-Schweregrad.

Um eine neue Regel zu erstellen, klicken Sie auf die Schaltfläche +. Doppelklicken Sie auf das Feld **Name** und geben Sie zur einfacheren Identifizierung eine Beschreibung der Regel ein.

Mit dem Kontrollkästchen des Felds **Aktiviert** kann die Regel aktiviert/deaktiviert werden. Dies kann hilfreich sein, wenn Sie eine Regel später verwenden und daher nicht dauerhaft löschen möchten.

**Typ**

**URL-basierte Aktion** - Zugriff auf die gegebene Website. Doppelklicken Sie auf das Feld **URL/ Kategorie** und geben Sie die entsprechende URL-Adresse ein.
In der Liste der URL-Adressen können Sie die Sonderzeichen * (Sternchen) und ? (Fragezeichen) nicht verwenden. Webseitenadressen mit mehreren TLDs (Top-Level-Domains) müssen zur erstellten Gruppe eingegeben werden (*beispielseite.com*, *beispielseite.sk* usw.). Wenn Sie eine Domäne zur Liste hinzufügen, werden alle Inhalte der Domäne und der Unterdomänen (z. B. *unterdomäne.beispielseite.com*) je nach gewählter URL-basierter Aktion gesperrt bzw. zugelassen.
**Kategorie-basierte Aktion** - Doppelklicken Sie auf das Feld **URL/Kategorie** und wählen Sie die Kategorien aus.

**Identität**

Hier können Sie Benutzer auswählen, auf die die Regel angewendet wird.

**Zugriffsrechte**

**Zulassen** - Auf die URL-Adresse/Kategorie darf zugegriffen werden.
**Sperren** - Sperrt die URL-Adresse/Kategorie.

**Schweregrad** (für das Filtern 26 der Log-Dateien)

**Immer** - Alle Ereignisse werden protokolliert.
**Diagnose** - Informationen, die für die Feineinstellung des Programms benötigt werden, werden protokolliert.
**Informationen** - Zeichnet zusätzlich zu den oben genannten Einträgen informative Meldungen auf.
**Warnungen** - Kritische Fehler und Warnungen werden protokolliert.
**Keine** - Es werden keine Logs erstellt.

## 11. Tools

Das Menü **Tools** enthält Module zur einfacheren Verwaltung des Programms und mit zusätzlichen Optionen für fortgeschrittene Benutzer.

### 11.1 Log-Dateien

Die Log-Dateien enthalten Informationen zu allen wichtigen aufgetretenen Programmereignissen und geben einen Überblick über erkannte Bedrohungen. Das Aufzeichnen von Logs ist unabdingbar für die Systemanalyse, die Erkennung von Problemen oder

Risiken sowie die Fehlerbehebung. Die Logs werden im Hintergrund ohne Eingriffe des Benutzers erstellt. Welche Informationen aufgezeichnet werden, ist abhängig von den aktuellen Einstellungen für die Mindestinformation in Logs. Textnachrichten und Logs können direkt aus ESET Endpoint Security heraus angezeigt werden. Das Archivieren von Logs erfolgt ebenfalls direkt über das Programm.

Log-Dateien können über das Hauptfenster von ESET Endpoint Security aufgerufen werden, indem Sie auf **Tools** > **Log-Dateien** klicken. Wählen Sie in der Liste **Log** im oberen Bereich des Fensters das gewünschte Log aus. Folgende Logs sind verfügbar:

1. **Erkannte Bedrohungen** – Informationen zu Ereignissen in Bezug auf erkannte Bedrohungen.
2. **Ereignisse** - Alle von ESET Endpoint Security ausgeführten wichtigen Aktionen werden in den Ereignis-Logs aufgezeichnet.
3. **Scannen des Computers** – In diesem Fenster werden die Ergebnisse aller durchgeführten Scans angezeigt. Durch Doppelklicken auf einen Eintrag können Sie Einzelheiten zu einem bestimmten Computer-Scan anzeigen.
4. **Medienkontrolle** - Enthält Einträge zu Wechselmedien oder externen Geräten, die an den Computer angeschlossen wurden. Nur Geräte mit einer Regel für die Medienkontrolle werden in die Log-Datei aufgenommen. Wenn auf ein angeschlossenes Gerät keine Regel zutrifft, wird für das Gerät kein Log-Eintrag erstellt. Hier können Sie außerdem Details wie Gerätetyp, Seriennummer, Herstellername und Mediengröße (je nach Verfügbarkeit der Informationen) anzeigen.
5. **Firewall** - Das Firewall-Log zeigt alle von der Personal Firewall entdeckten Angriffe von anderen Computern an. Firewall-Logs enthalten Informationen zu erkannten Systemangriffen. In der Spalte **Ereignis** werden die erkannten Angriffe aufgelistet. Die Spalte **Quelle** enthält weitere Informationen über den Angreifer und die Spalte **Protokoll** gibt an, welches Kommunikationsprotokoll für den Angriff verwendet wurde.
6. **Web-Kontrolle** - Zeigt gesperrte bzw. zugelassene URL-Adressen und Details zu deren Kategorien an.
7. **Gefilterte Websites** - Diese Liste enthält die durch den Web-Schutz 18 oder die Web-Kontrolle 24 gesperrten Websites. Die Logs enthalten die Uhrzeit, die URL, den Status, die IP-Adresse, den Benutzer und die Anwendung, die eine Verbindung zur gegebenen Website hergestellt hat.

Klicken Sie mit der rechten Maustaste auf eine beliebige Log-Datei und klicken Sie dann auf **Kopieren**, um den Inhalt dieser Log-Datei in die Zwischenablage zu kopieren.

### 11.1.1 Log-Wartung

Die Log-Konfiguration für ESET Endpoint Security können Sie aus dem Hauptprogrammfenster aufrufen. Klicken Sie auf **Einstellungen** > **Erweiterte Einstellungen** > **Tools** > **Log-Dateien**. Für Log-Dateien können die folgenden Einstellungen vorgenommen werden:

- **Alte Log-Einträge automatisch löschen** – Log-Einträge, die älter als die angegebene Anzahl Tage sind, werden automatisch gelöscht.
- **Log-Dateien automatisch optimieren** – Die Logs werden beim Erreichen des vordefinierten Fragmentierungsgrads automatisch optimiert.

Alle relevanten Informationen in der grafischen Benutzeroberfläche sowie Bedrohungs- und Ereignisnachrichten können in menschenlesbarer Textform gespeichert werden, z. B. in Nur-Text- oder CSV-Dateien (durch Komma getrennte Dateien). Wenn Sie diese Dateien zur weiteren Verarbeitung in Drittanbieter-Tools verfügbar machen möchten, aktivieren Sie das Kontrollkästchen neben **Protokollierung in Textdateien aktivieren**.

Um den Zielordner für die Log-Dateien festzulegen, klicken Sie auf **Einstellungen** neben **Erweiterte Einstellungen**.

Je nach den unter **Textprotokolldateien: Bearbeiten** ausgewählten Optionen, können Log-Dateien mit folgenden Informationen gespeichert werden:

- Ereignisse wie *Ungültiger Benutzername/ungültiges Passwort*, *Signaturdatenbank konnte nicht aktualisiert werden* usw. werden in der Datei *eventslog.txt* gespeichert.
- Durch den Systemstart-Scanner, den Echtzeit-Dateischutz oder den Computerscan erkannte Bedrohungen werden in der Datei *threatslog.txt* gespeichert.
- Die Ergebnisse aller durchgeführten Scans werden im Format *scanlog.NUMBER.txt* gespeichert.
- Von der Medienkontrolle blockierte Geräte werden in devctllog.txt aufgezeichnet.
- Alle Ereignisse in Bezug auf die Kommunikation über die Firewall werden in die Datei firewalllog.txt geschrieben.
- Von der Web-Kontrolle blockierte Seiten werden in webctllog.txt aufgezeichnet.

Um die **Standardcomputer-Scanprotokolleinträge** zu konfigurieren, klicken Sie auf **Bearbeiten** und aktivieren/deaktivieren die einzelnen Log-Typen je nach Bedarf. Weitere Erläuterungen zu diesen Log-Typen finden Sie unter Log-Filter 26.

### 11.1.2 Log-Filter

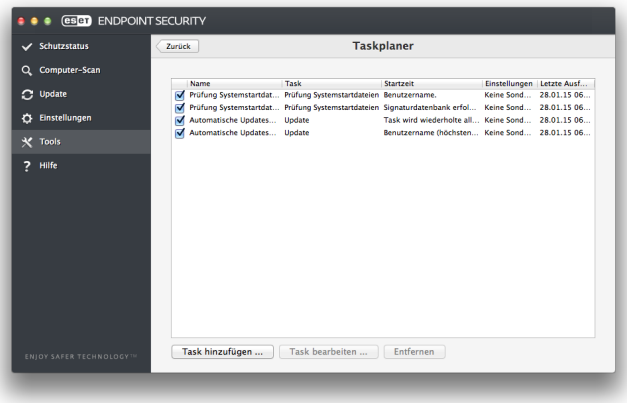
In den Logs werden Informationen über wichtige Systemereignisse gespeichert: Mit dem Log-Filter können Sie Einträge zu bestimmten Ereignissen anzeigen.

Nachfolgend sind die am häufigsten verwendeten Arten von Logs aufgelistet:

- **Kritische Warnungen** – kritische Systemfehler (z. B. „Virenschutz konnte nicht gestartet werden“)
- **Fehler** - Fehler wie *„Fehler beim Herunterladen einer Datei“* und kritische Fehler
- **Warnungen** – Warnmeldungen
- **Informationen** - Meldungen wie erfolgreiche Updates oder Warnungen
- **Diagnosedaten** – alle bisher genannten Einträge sowie Informationen, die für die Feineinstellung des Programms erforderlich sind

## 11.2 Taskplaner

Um den Taskplaner zu öffnen, klicken Sie im Hauptmenü von ESET Endpoint Security unter **Tools** auf **Taskplaner**. Der **Taskplaner** umfasst eine Liste aller geplanten Tasks sowie deren Konfigurationseigenschaften, inklusive des vordefinierten Datums, der Uhrzeit und des verwendeten Scanprofils.




Der Taskplaner verwaltet und startet Tasks mit vordefinierter Konfiguration und voreingestellten Eigenschaften. Konfiguration und Eigenschaften enthalten Informationen wie Datum und Uhrzeit und bestimmte Profile, die bei Ausführung des Tasks verwendet werden.

Standardmäßig werden im Taskplaner die folgenden Tasks angezeigt:

- Log-Wartung (nach Aktivieren von **System-Tasks anzeigen** in den Taskplaner-Einstellungen)
- Prüfung Systemstartdateien nach Anmeldung des Benutzers
- Prüfung Systemstartdateien nach Update der Signaturdatenbank
- Automatische Updates in festen Zeitabständen
- Automatische Updates beim Anmelden des Benutzers

Um die Konfiguration eines vorhandenen Standardtasks oder eines benutzerdefinierten Tasks zu ändern, halten Sie die Ctrl-Taste gedrückt und klicken Sie auf den Task und dann auf **Bearbeiten**. Alternativ können Sie den Task, den Sie ändern möchten, auswählen und dann auf **Task bearbeiten** klicken.

### 11.2.1 Erstellen von Tasks

Zum Erstellen eines neuen Tasks im Taskplaner klicken Sie auf **Task hinzufügen** oder halten die Strg-Taste gedrückt, klicken auf das leere Feld und wählen dann im Kontextmenü die Option **Hinzufügen** aus. Es gibt fünf Arten von Tasks:

- **Anwendung starten**
- **Update**
- **Log-Wartung**
- **On-Demand-Scan**
- **Prüfung der Systemstartdateien**

**HINWEIS:** Wenn Sie **Anwendung ausführen** auswählen, können Sie Programme mit dem Systembenutzer „nobody“ („niemand“) ausführen. Die Berechtigungen zum Ausführen von Anwendungen über den Taskplaner werden über Mac OS X definiert.

Im nachfolgenden Beispiel wird über den Taskplaner ein neues Update-Task hinzugefügt (Updates stellen die am häufigsten geplanten Tasks dar):

1. Wählen Sie im Dropdownmenü **Geplanter Task** die Option **Update** aus.
2. Geben Sie im Feld **Taskname** einen Namen für den Task ein.

3. Wählen Sie in der Liste **Task ausführen** das gewünschte Ausführungsintervall. Je nach ausgewähltem Intervall werden Sie aufgefordert, verschiedene Update-Parameter festzulegen. Bei der Auswahl von **Benutzerdefiniert** werden Sie aufgefordert, Datum und Uhrzeit im *cron*-Format anzugeben (nähere Informationen finden Sie im Abschnitt Erstellen eines benutzerdefinierten Tasks 27).
4. Im nächsten Schritt legen Sie eine Aktion für den Fall fest, dass der Task zur geplanten Zeit nicht ausgeführt oder abgeschlossen werden kann.
5. Klicken Sie auf **Fertig stellen**. Der neue geplante Task wird der Liste der aktuellen Tasks hinzugefügt.

Einige Tasks sind für die ordnungsgemäße Funktion des Systems unerlässlich und standardmäßig in ESET Endpoint Security enthalten. Diese System-Tasks sollten nicht modifiziert werden. Die Anzeige ist standardmäßig ausgeschaltet. Um diese Tasks anzuzeigen, klicken Sie im Hauptmenü auf **Einstellungen** > **Erweiterte Einstellungen** > **Taskplaner** und wählen Sie **System-Tasks anzeigen** aus.

### 11.2.2 Erstellen eines benutzerdefinierten Tasks

Wenn Sie im Dropdown-Menü „Task ausführen“ den Tasktyp „Benutzerdefiniert“ auswählen, müssen Sie einige Parameter definieren.

Datum und Uhrzeit von Tasks des Typs **Benutzerdefiniert** müssen im cron-Langformat mit Jahr angegeben werden (Zeichenfolge aus 6 Feldern, jeweils getrennt durch ein Leerraumzeichen):

```
Minute(0-59) Stunde(0-23) Tag(1-31) Monat(1-12) Jahr(1970-2099) Wochentag(0-7)(Sonntag = 0 oder 7)
```

Beispiel:

```
30 6 22 3 2012 4
```

Folgende Sonderzeichen werden in cron-Ausdrücken unterstützt:

- Sternchen (`*`) - Steht für alle möglichen Werte des betreffenden Felds. Beispiel: Sternchen im dritten Feld (Tag) = jeder Tag im Monat
- Bindestrich (`-`) - Definition von Zeiträumen, z. B. `3-9`
- Komma (`,`) - Trennt mehrere Einträge einer Liste, z. B. `1,3,7,8`
- Schrägstrich (`/`) - Definition von Intervallen in Zeiträumen. Beispiel: `3-28/5` im dritten Feld (Tag) = am 3. des Monats und anschließend alle 5 Tage.

Textbezeichnungen für Tage (Monday-Sunday) und Monate (January-December) werden nicht unterstützt.

**HINWEIS:** Werden sowohl Tag als auch Wochentag angegeben, so wird der Befehl nur ausgeführt, wenn beide Bedingungen erfüllt sind.

## 11.3 Live Grid

Dank des Live Grid-Frühwarnsystems erhält ESET unmittelbar und fortlaufend aktuelle Informationen zu neuen Infiltrationen. Das Live Grid-Frühwarnsystem funktioniert in zwei Richtungen, hat jedoch nur einen Zweck: die Verbesserung des Schutzes, den wir Ihnen bieten. Die einfachste Möglichkeit, neue Bedrohungen zu erkennen, sobald sie in Erscheinung treten, besteht darin, so viele unserer Kunden wie möglich einzubinden und die von ihnen erfassten Informationen zur Aktualisierung der Signaturinformationen zu nutzen. Wählen Sie eine der beiden Optionen für Live Grid:

1. Sie können sich entscheiden, das Live Grid-Frühwarnsystem nicht zu aktivieren. Die Funktionalität in der Software geht nicht verloren, in einigen Fällen reagiert ESET Endpoint Security jedoch möglicherweise schneller auf neue Bedrohungen als die Aktualisierung der Signaturdatenbank.
2. Sie können das Live Grid-Frühwarnsystem so konfigurieren, dass Informationen über neue Bedrohungen und Fundstellen von gefährlichem Code übermittelt werden. Die Informationen bleiben anonym. Diese Informationen können zur detaillierten Analyse an ESET gesendet werden. Nach ihrer Untersuchung kann ESET dann die Signaturdatenbank aktualisieren und so die Erkennungsleistung des Programms verbessern.

Das Live Grid-Frühwarnsystem sammelt Daten über neue Bedrohungen, die auf Ihrem Computer erkannt wurden. Dazu können auch Proben oder Kopien der Datei gehören, in der eine Bedrohung aufgetreten ist, der Pfad zu dieser Datei, der Dateiname, Datum und Uhrzeit, der Prozess, über den die Bedrohung auf Ihrem Computer in Erscheinung getreten ist, und Informationen zum Betriebssystem des Computers.

Auch wenn es möglich ist, dass das ESET-Virenlabor auf diese Weise gelegentlich einige Informationen über Sie oder Ihren Computer erhält (zum Beispiel Benutzernamen in einem Verzeichnispfad usw.), werden diese Daten für keinen anderen Zweck als zur Verbesserung der unmittelbaren Reaktion auf neue Bedrohungen verwendet.

Zum Zugriff auf die Live Grid-Einrichtung klicken Sie im Hauptmenü auf **Einstellungen** > **Erweiterte Einstellungen** > **Live Grid**. Wählen Sie **An ESET Live Grid teilnehmen (empfohlen)** aus, um Live Grid zu aktivieren. Klicken Sie dann neben **Erweiterte Einstellungen** auf **Einstellungen**.

### 11.3.1 Verdächtige Dateien

ESET Endpoint Security ist standardmäßig so konfiguriert, dass verdächtige Dateien zur genauen Analyse an das ESET-Virenlabor eingereicht werden. Wenn Sie die Dateien nicht automatisch einreichen möchten, deaktivieren Sie **Einreichen verdächtiger Dateien** (**Einstellungen** > **Erweiterte Einstellungen** > **Live Grid** > **Einstellungen**).

Wenn Sie eine verdächtige Datei finden, können Sie sie zur Analyse an unser Virenlabor einreichen. Klicken Sie hierzu im Hauptprogrammfenster auf **Tools** > **Datei zur Analyse einreichen**. Sollte dabei schädlicher Code zutage treten, wird die entsprechende Signatur beim nächsten Update der Signaturdatenbank berücksichtigt.

**Anonymisierte statistische Daten einreichen** - Das ESET Live Grid-Frühwarnsystem erfasst anonyme Informationen zu Ihrem Computer in Bezug auf neu erkannte Bedrohungen. Erfasst werden der Name der Bedrohung, Datum und Uhrzeit der Erkennung, die Versionsnummer des ESET Security-Produkts sowie Versionsdaten und die Regionaleinstellung des Betriebssystems. Diese Statistikpakete werden normalerweise einmal oder zweimal täglich an ESET übermittelt.

Beispiel für ein typisches Statistikpaket:

```
# utc_time=2005-04-14 07:21:28
# country="Slovakia"
# language="ENGLISH"
# osver=9.5.0
# engine=5417
# components=2.50.2
# moduleid=0x4e4f4d41
# filesize=28368
# filename=Users/UserOne/Documents/Incoming/
rdgFR1463[1].zip
```

**Ausschlussfilter** – Über diese Option können Sie bestimmte Dateitypen vom Senden ausschließen. Hier können Dateien eingetragen werden, die eventuell vertrauliche Informationen enthalten, wie zum Beispiel Textdokumente oder Tabellen. Die üblichsten Dateitypen sind bereits in der Standardeinstellung in die Liste eingetragen (.doc, .rtf usw.). Sie können der Ausschlussliste weitere Dateitypen hinzufügen.

**E-Mail-Adresse für Rückfragen (optional)** - Ihre E-Mail-Adresse kann dazu verwendet werden, Sie bei Rückfragen zu kontaktieren. Beachten Sie, dass Sie nur dann eine Antwort von ESET erhalten, wenn weitere Informationen von Ihnen benötigt werden.

## 11.4 Quarantäne

Hauptzweck der Quarantäne ist die sichere Verwahrung infizierter Dateien. Dateien sollten in die Quarantäne verschoben werden, wenn sie nicht gesäubert werden können, wenn es nicht sicher oder ratsam ist, sie zu löschen, oder wenn sie von ESET Endpoint Security fälschlicherweise erkannt worden sind.

Sie können beliebige Dateien gezielt in die Quarantäne verschieben. Geschehen sollte dies bei Dateien, die sich verdächtig verhalten, während des Virenschutz-Scans jedoch nicht erkannt werden. Dateien aus der Quarantäne können zur Analyse an das ESET-Virenlabor eingereicht werden.

Die Dateien im Quarantäneordner können in einer Tabelle angezeigt werden, die Datum und Uhrzeit der Quarantäne, den Pfad zum ursprünglichen Speicherort der infizierten Datei, ihre Größe in Byte, einen Grund (z. B. Objekt hinzugefügt durch Benutzer) und die Anzahl der erkannten Bedrohungen enthält. Der Quarantäneordner (*/Library/Application Support/Eset/esets/cache/quarantine*) bleibt auch nach der Deinstallation von ESET Endpoint Security im System bestehen. Die Quarantänedateien werden sicher verschlüsselt gespeichert und können nach der Reinstallation von ESET Endpoint Security wiederhergestellt werden.

### 11.4.1 Quarantäne für Dateien

ESET Endpoint Security kopiert gelöschte Dateien automatisch in den Quarantäneordner (sofern diese Option nicht im Warnfenster deaktiviert wurde). Im Fenster „Quarantäne“ können Sie auf „Quarantäne“ klicken, um eine Datei manuell zur Quarantäne hinzuzufügen. Sie können auch jederzeit bei gedrückter Strg-Taste auf eine Datei klicken und im Kontextmenü „Dienste“ > „ESET Endpoint Security - Dateien zur Quarantäne hinzufügen“ auswählen, um eine Datei in die Quarantäne zu verschieben.

### 11.4.2 Wiederherstellen einer Datei aus der Quarantäne

Dateien können aus der Quarantäne an ihrem ursprünglichen Speicherort wiederhergestellt werden. Wählen Sie hierzu eine Datei aus und klicken Sie auf **Wiederherstellen**. Die Wiederherstellungsfunktion ist auch über das Kontextmenü verfügbar. Halten Sie die Strg-Taste gedrückt und klicken Sie auf die gewünschte Datei im Quarantänefenster. Klicken Sie dann auf **Wiederherstellen**. Über die Funktion **Wiederherstellen nach** können Sie eine Datei an einem anderen als dem ursprünglichen Speicherort wiederherstellen.

### 11.4.3 Einreichen von Dateien aus der Quarantäne

Wenn Sie eine verdächtige, nicht vom Programm erkannte Datei in Quarantäne versetzt haben oder wenn eine Datei fälschlich als infiziert eingestuft wurde (etwa durch die heuristische Analyse des Codes) und infolgedessen in den Quarantäneordner verschoben wurde, senden Sie die Datei zur Analyse an das ESET-Virenlabor. Um eine Datei zu senden, die in der Quarantäne gespeichert ist, drücken Sie die Strg-Taste und klicken Sie auf die Datei. Wählen Sie dann im angezeigten Kontextmenü die Option **Datei zur Analyse einreichen** aus.

## 11.5 Berechtigungen

Die Einstellungen von ESET Endpoint Security können im Hinblick auf die Sicherheitsrichtlinien Ihres Unternehmens von großer Wichtigkeit sein. Unbefugte Änderungen können die Stabilität und den Schutz Ihres Systems gefährden. Deshalb können Sie auswählen, welche Benutzer die Programmkonfiguration bearbeiten dürfen.

Sie können privilegierte Benutzer unter **Einstellungen** > **Erweiterte Einstellungen** > **Benutzer** > **Rechte** konfigurieren.

Maßgeblich für einen wirksamen Schutz Ihres Systems ist die richtige Konfiguration des Programms. Bei unzulässigen Änderungen können wichtige Daten verloren gehen. Um die Liste der privilegierten Benutzer einzurichten, wählen Sie die gewünschten Benutzer links in der Liste **Benutzer** aus und klicken auf **Hinzufügen**. Um einen Benutzer zu entfernen, wählen Sie ihn in der Liste **Privilegierte Benutzer** rechts aus und klicken auf **Entfernen**. Um alle Systembenutzer anzuzeigen, wählen Sie die Option **Alle Benutzer anzeigen** aus.

**HINWEIS:** Wenn die Liste der privilegierten Benutzer leer ist, können alle Systembenutzer die Programmeinstellungen bearbeiten.

## 11.6 Präsentationsmodus

Der **Präsentationsmodus** ist eine Funktion für Benutzer, die ihre Software ununterbrochen nutzen, nicht durch Popup-Fenster gestört werden und die CPU-Auslastung reduzieren möchten. Der Präsentationsmodus kann auch während Präsentationen verwendet werden, die nicht durch eine Aktion des Virenschutzes unterbrochen werden dürfen. Wenn er aktiviert ist, werden alle Popup-Fenster deaktiviert und geplante Tasks werden nicht ausgeführt. Der Systemschutz läuft weiter im Hintergrund, doch es sind keine Eingaben durch Benutzer erforderlich.

Um den Präsentationsmodus manuell zu aktivieren, klicken Sie auf **Einstellungen** > **Erweiterte Einstellungen ...** > **Präsentationsmodus** > **Präsentationsmodus aktivieren**.

Aktivieren Sie das Kontrollkästchen neben **Präsentationsmodus im Vollbildmodus automatisch aktivieren**, wenn der Präsentationsmodus beim Ausführen von Anwendungen im Vollbildmodus automatisch ausgelöst werden soll. Wenn diese Funktion aktiviert ist, wird der Präsentationsmodus gestartet, sobald Sie eine Vollbildanwendung initiieren, und automatisch beendet, wenn Sie diese Vollbildanwendung beenden. Dies ist besonders zum Beginnen einer Präsentation hilfreich.

Mit der Option **Präsentationsmodus automatisch deaktivieren nach** können Sie außerdem die Zeit in Minuten festlegen, nach der der Präsentationsmodus automatisch deaktiviert wird.

Im Präsentationsmodus besteht ein erhöhtes Risiko. Daher wird das Schutzstatus-Symbol von ESET Endpoint Security orange und mit einer Warnung angezeigt.

**HINWEIS:** Wenn für die Personal Firewall der interaktive Filtermodus eingestellt und der Präsentationsmodus aktiviert ist, kann es zu Problemen beim Aufbau einer Internetverbindung kommen. Dies kann beim Ausführen einer Awendung, die eine Internetverbindung verwendet, zu Problemen führen. Üblicherweise müssen Sie eine solche Aktion bestätigen (sofern keine Verbindungsregeln oder -ausnahmen festgelegt wurden), doch im Präsentationsmodus kann der Benutzer keine derartigen Eingaben machen. Um dies zu umgehen, muss entweder eine Verbindungsregel für jede Anwendung festgelegt werden, mit der es im Präsentationsmodus zu Konflikten kommen kann, oder es muss eine andere Filtermethode für die Personal Firewall gewählt werden. Bedenken Sie, dass Sie im Präsentationsmodus bei dem Versuch, eine Website zu besuchen oder eine Anwendung auszuführen, die möglicherweise Sicherheitsrisiken darstellen, nicht benachrichtigt bzw. gewarnt werden, dass diese blockiert sind. Grund dafür ist die deaktivierte Benutzerinteraktion.

### 11.7 Ausgeführte Prozesse

Die Liste **Ausgeführte Prozesse** zeigt die auf Ihrem Computer ausgeführten Prozesse an. ESET Endpoint Security liefert detaillierte Informationen zu den ausgeführten Prozessen, um Benutzern den Schutz der ESET Live Grid-Technologie zu bieten.

- **Prozess** - Name des aktuell auf Ihrem Computer ausgeführten Prozesses. Sie können die auf dem Computer ausgeführten Prozesse auch mit der Aktivitätsanzeige (*/Applications/Utilities*) anzeigen.
- **Risikostufe** - In den meisten Fällen weisen ESET Endpoint Security und die ESET Live Grid-Technologie den Objekten (Dateien, Prozesse usw.) eine Risikostufe zu. Dies erfolgt unter Einsatz einer Reihe heuristischer Regeln, die die Eigenschaften des Objekts untersuchen und auf dieser Grundlage den Verdacht auf Schadcode abwägen. Den Objekten wird auf Grundlage dieser heuristischen Regeln eine Risikostufe zugewiesen. Bekannte Anwendungen, die grün markiert und bekanntermaßen keinen Schadcode enthalten (Positivliste), werden von der Prüfung ausgeschlossen. Dies sorgt für schnellere On-Demand- und Echtzeit-Scans. Eine als unbekannt eingestufte Anwendung (gelb) enthält nicht unbedingt Schadcode. Meist handelt es sich einfach um eine neuere Anwendung. Wenn Sie sich bei einer Datei nicht sicher sind, können Sie sie zur Analyse an das ESET-Virenlabor einreichen. Wenn sich herausstellt, dass die Datei Schadcode enthält, wird die entsprechende Signatur zu einem zukünftigen Update hinzugefügt.
- **Anzahl Benutzer** - gibt die Anzahl der Benutzer an, die eine bestimmte Anwendung verwenden. Diese Information wird durch die ESET Live Grid-Technologie erfasst.
- **Erkennungszeit** - gibt an, wann die Anwendung von der ESET Live Grid-Technologie erkannt wurde.
- **Anwendungspaket-ID** - Name des Herstellers oder des Anwendungsprozesses.

Wenn Sie auf einen Prozess klicken, werden am unteren Bildschirmrand folgende Informationen angezeigt:

- **Datei** - Speicherort der Anwendung auf Ihrem Computer
- **Dateigröße** - physikalische Größe der Datei auf dem Datenträger
- **Dateibeschreibung** - Dateieigenschaften auf Grundlage der Beschreibung vom Betriebssystem
- **Anwendungspaket-ID** - Name des Herstellers oder des Anwendungsprozesses.

- **Dateiversion** - Informationen vom Herausgeber der Anwendung
- **Produktname** - Anwendungs- und/oder Firmenname

# 12. Benutzeroberfläche

Über die Konfigurationsoptionen für die Benutzeroberfläche können Sie die Arbeitsumgebung an Ihre Anforderungen anpassen. Diese Optionen sind unter **Einstellungen** > **Erweiterte Einstellungen** > **Benutzeroberfläche** verfügbar.

- Um das ESET Endpoint Security-Startbild beim Programmstart zu aktivieren, aktivieren Sie die Option **Startbild anzeigen**.
- Die Option **Anwendung in Dock anzeigen** bewirkt, dass das ESET Endpoint Security-Symbol im Mac OS-Dock angezeigt wird und dass Sie mit der Tastenkombination *cmd-tab* zwischen ESET Endpoint Security und anderen geöffneten Anwendungen wechseln können. Die Änderungen werden beim nächsten Start von ESET Endpoint Security (in der Regel nach einem Neustart des Computers) wirksam.
- Wenn Sie **Standardmenü verwenden** aktivieren, können Sie bestimmte Tastaturbefehle 10 verwenden und Standardmenüeinträge in der Mac OS-Menüleiste (oben am Bildschirm) anzeigen.
- Aktivieren Sie **QuickInfo anzeigen**, damit QuickInfos angezeigt werden, wenn der Cursor über bestimmte Optionen von ESET Endpoint Security bewegt wird.
- Wenn **Versteckte Dateien anzeigen** aktiviert ist, können Sie im Einstellungsbereich **Zu scannende Objekte** der Funktion **Computer scannen** auch versteckte Dateien sehen und diese auswählen.

## 12.1 Warnungen und Benachrichtigungen

Im Bereich **Warnungen und Benachrichtigungen** können Sie konfigurieren, wie Warnungen und Systembenachrichtigungen in ESET Endpoint Security behandelt werden.

Wenn Sie die Option **Warnungen anzeigen** deaktivieren, werden keinerlei Warnfenster angezeigt. Dies wird nur für bestimmte Situationen empfohlen. Für die meisten Benutzer empfiehlt es sich, die Standardeinstellung (aktiviert) beizubehalten.

Wenn Sie **Hinweise auf dem Desktop anzeigen** auswählen, werden Warnfenster, die keinen Benutzereingriff erfordern, auf dem Desktop angezeigt (standardmäßig oben rechts auf dem Bildschirm). Wie lang solche Benachrichtigungen angezeigt werden, können Sie über den Wert **Hinweise automatisch schließen nach** X **Sekunden** festlegen.

### 12.1.1 Erweiterte Einstellungen für Warnungen und Benachrichtigungen

Bei neuen Programmversionen und Betriebssystem-Updates, beim Deaktivieren bestimmter Programmkomponenten, beim Löschen von Logs usw. werden in ESET Endpoint Security Warnfenster angezeigt. Sie können die einzelnen Benachrichtigungen mit Wirkung für die Zukunft unterdrücken, indem Sie **Dialogfenster nicht mehr anzeigen** auswählen.

Unter **Liste der Dialogfenster** (**Einstellungen** > **Erweiterte Einstellungen** > **Warnungen und Benachrichtigungen** > **Einstellungen**) finden Sie eine Liste all dieser Warn- und Benachrichtigungsdialoge in ESET Endpoint Security. Über das Kontrollkästchen neben **Dialogname** können Sie die Anzeige der einzelnen Benachrichtigungsarten aktivieren oder unterdrücken. Außerdem können Sie **Anzeigebedingungen** für Hinweise zu neuen Programmversionen und Betriebssystem-Updates definieren.

## 12.2 Kontextmenü

Um Funktionen von ESET Endpoint Security im Kontextmenü verfügbar zu machen, klicken Sie auf **Einstellungen** > **Erweiterte Einstellungen** > **Kontextmenü** und aktivieren Sie das Kontrollkästchen neben **In Kontextmenü integrieren**. Die Änderungen werden nach dem Abmelden und einem Neustart des Computers übernommen. Die Optionen des Kontextmenüs werden auf dem Desktop im **Finder**-Fenster angezeigt, wenn Sie bei gedrückter STRG-Taste auf eine beliebige Datei klicken.

# 13. Update

Für optimalen Schutz muss ESET Endpoint Security regelmäßig aktualisiert werden. Die Updates für die Signaturdatenbank halten das Programm fortlaufend auf dem neuesten Stand.

Über **Update** im Hauptmenü können Sie sich den aktuellen Update-Status anzeigen lassen. Hier sehen Sie Datum und Uhrzeit des letzten Updates und können feststellen, ob ein Update erforderlich ist. Um ein Update manuell zu starten, klicken Sie auf **Signaturdatenbank aktualisieren**.

Wenn beim Update-Download keinerlei Zwischenfälle auftreten und Sie über die neueste Signaturdatenbank verfügen, wird im Update-Fenster der Hinweis *Update nicht erforderlich - die Signaturdatenbank ist auf dem neuesten Stand* angezeigt. Wenn das Update der Signaturdatenbank fehlschlägt, sollten Sie die Update-Einstellungen 32 überprüfen. Die häufigste Fehlerursache sind falsch eingegebene Lizenzdaten 9 oder fehlerhaft konfigurierte Verbindungseinstellungen 34.

Im Fenster **Update** wird auch die Versionsnummer der Signaturdatenbank angezeigt. Die Versionsnummer ist ein aktiver Link zur ESET-Website, wo alle im gegebenen Update hinzugefügten Signaturen angezeigt werden.

## 13.1 Einstellungen für Updates

In den Einstellungen für Updates finden Sie Informationen zum Abruf von Updates, z. B. die Liste der Update-Server und die Lizenzdaten für diese Server. Standardmäßig ist die Option **Update-Server** auf **Automatisch auswählen** eingestellt. So werden Updates automatisch von dem ESET-Server heruntergeladen, der am wenigsten belastet ist.

Die Liste **Update-Server** zeigt eine Aufstellung der aktuellen Update-Server. Um einen neuen Update-Server hinzuzufügen, klicken Sie auf **Bearbeiten**, geben Sie die Adresse des neuen Servers in das Eingabefeld **Update-Server** ein und klicken Sie auf **Hinzufügen**.

In ESET Endpoint Security haben Sie die Möglichkeit, einen alternativen Update-Server oder Failover-Update-Server festzulegen. Beispielsweise könnten Sie unter **Primärer Server** Ihren Mirror-Server und unter **Sekundär Server** den normalen ESET-Update-Server festlegen. Der sekundäre Server wird nur verwendet, wenn sich diese beiden Angaben unterscheiden. Wenn Sie die Angaben für den sekundären Server (Update-Server, Benutzername, Passwort) leer lassen, kann natürlich auch kein Update über einen sekundären Server durchgeführt werden. Wenn Sie „Automatisch auswählen“ aktivieren und Ihren Benutzernamen und das Passwort in die entsprechenden Felder eingeben, wählt ESET Endpoint Security automatisch den am besten geeigneten Update-Server aus.

Wenn beim Herunterladen der Updates für die Signaturdatenbank Fehler auftreten, klicken Sie auf **Update Cache löschen**, um temporäre Update-Dateien zu löschen.

### 13.1.1 Erweiterte Einstellungen

Um die Benachrichtigungen zu erfolgreichen Updates zu deaktivieren, wählen Sie **Keine Benachrichtigung über erfolgreiche Updates anzeigen** aus.

Aktivieren Sie den Testmodus, um Entwicklungsmodule herunterzuladen, die sich in der abschließenden Testphase befinden. Die Updates des Testmodus enthalten Korrekturen für Produktprobleme. Mit dem verzögerten Update werden die Updates einige Stunden nach ihrer Veröffentlichung heruntergeladen, um sicherzustellen, dass die Clients die Updates erst erhalten, wenn bestätigt ist, dass keine Probleme mit den Updates auftreten.

ESET Endpoint Security zeichnet Snapshots der Signaturdatenbank und der Programmmodule zur späteren Verwendung mit der **Update-Rollback**-Funktion auf. Lassen Sie **Snapshots der Update-Dateien erstellen** aktiviert, damit ESET Endpoint Security diese Snapshots automatisch aufzeichnet. Wenn Sie befürchten, dass ein neues Update der Signaturdatenbank oder eines Programmmoduls korrupt oder nicht stabil ist, können Sie einen Rollback zur vorigen Version ausführen und Updates für einen bestimmten Zeitraum deaktivieren. Hier können Sie auch zuvor für einen unbegrenzten Zeitraum deaktivierte Updates wieder aktivieren. Wenn Sie ein Rollback zu einem früheren Update ausführen, legen Sie im Dropdown-Menü „Dauer für Aussetzen festlegen auf“ den Zeitraum fest, für den die Updates ausgesetzt werden sollen. Wenn Sie „Bis zur Aufhebung“ auswählen, werden die normalen Updates erst fortgesetzt, wenn Sie dies manuell wiederherstellen. Verwenden Sie diese Option mit Vorsicht.

**Maximales Datenbankalter automatisch festlegen** Hier können Sie eine Zeitdauer (in Tagen) festlegen, nach der die Signaturdatenbank spätestens als veraltet gemeldet wird. Der Standardwert ist 7 Tage.

### 13.2 So erstellen Sie Update-Tasks

Klicken Sie auf „Update“ > **Update der Signaturdatenbank**, um manuell ein Update der Signaturdatenbank auszulösen.

Darüber hinaus können Sie Updates auch als geplante Tasks einrichten. Um einen Task zu konfigurieren, klicken Sie auf **Tools** > **Taskplaner**. Standardmäßig sind in ESET Endpoint Security folgende Tasks aktiviert:

- **Automatische Updates in festen Zeitabständen**
- **Automatische Updates beim Anmelden des Benutzers**

Diese Update-Tasks können bei Bedarf bearbeitet werden. Neben den standardmäßig ausgeführten Update-Tasks können zusätzliche Update-Tasks mit benutzerdefinierten Einstellungen erstellt werden. Weitere Informationen zum Erstellen und Konfigurieren von Update-Tasks finden Sie unter Taskplaner 26.

### 13.3 Upgrade auf ein neues Build

Um maximalen Schutz zu gewährleisten, ist es wichtig, immer das neueste Build von ESET Endpoint Security zu verwenden. Klicken Sie auf **Update** im Hauptmenü links, um zu prüfen, ob eine neue Version verfügbar ist. Ist ein neues Build verfügbar, wird unten im Fenster eine Benachrichtigung angezeigt. Klicken Sie auf **Mehr Informationen**, um ein neues Fenster mit der Versionsnummer des neuen Builds und dem Änderungsprotokoll anzuzeigen.

Klicken Sie auf **Herunterladen**, um das neueste Build herunterzuladen. Klicken Sie auf **Schließen**, um das Fenster zu schließen und das Upgrade später herunterzuladen.

Wenn Sie auf **Herunterladen** geklickt haben, wird die Datei heruntergeladen und in Ihrem Download-Ordner (oder in dem von Ihrem Browser festgelegten Standardordner) abgelegt. Führen Sie nach Abschluss des Downloads die Datei aus und folgen Sie den Installationsanweisungen. Ihre Lizenzinformationen werden automatisch bei der neuen Installation übernommen.

Es wird empfohlen, regelmäßig zu prüfen, ob Upgrades verfügbar sind, insbesondere wenn ESET Endpoint Security von einer CD/DVD installiert wird.

### 13.4 Systemupdates

Die Systemupdatefunktion für Mac OS X ist eine wichtige Komponente zum Schutz des Benutzers vor Schadcode. Zur Gewährleistung des bestmöglichen Schutzes empfehlen wird, die Updates möglichst umgehend zu installieren, sobald sie verfügbar sind. ESET Endpoint Security zeigt je nach Wichtigkeit der Updates Benachrichtigungen zu fehlenden Updates an. Sie können festlegen, ab welcher Wichtigkeit Update-Benachrichtigungen angezeigt werden. Navigieren Sie hierzu zu **Einstellungen** > **Erweiterte Einstellungen** > **Warnungen und Benachrichtigungen > Einstellungen** und verwenden Sie das Dropdown-Menü **Anzeigebedingungen** neben **Betriebssystem-Updates**.

- **Alle Updates anzeigen** - Benachrichtigungen werden für alle fehlenden Updates angezeigt.
- **Nur empfohlene Updates anzeigen** - Benachrichtigungen werden nur für empfohlene Updates angezeigt.

Wenn Sie keine Benachrichtigungen zu fehlenden Updates erhalten möchten, deaktivieren Sie das Kontrollkästchen neben **Betriebssystem-Updates**.

Das Benachrichtigungsfenster enthält eine Übersicht der verfügbaren Updates für das Mac OS X-Betriebssystem und für die Anwendungen, die über das native Mac OS X-Tool für Software-Updates aktualisiert werden. Sie können das Update direkt über das Benachrichtigungsfenster ausführen oder über die **Startseite** von ESET Endpoint Security, indem Sie hier auf **Fehlendes Update installieren** klicken.

Das Benachrichtigungsfenster enthält den Anwendungsnamen, die Version, die Größe, Eigenschaften (Flags) und zusätzliche Informationen zu den verfügbaren Updates. Die Spalte **Flags** enthält folgende Informationen:

- **[empfohlen]** - Der Hersteller des Betriebssystem empfiehlt die Installation dieses Updates, um die Sicherheit und Stabilität des Systems zu verbessern.
- **[Neustart]** - Nach der Installation ist ein Neustart des Computers erforderlich.
- **[Herunterfahren]** - Der Computer muss heruntergefahren und nach der Installation wieder eingeschaltet werden.

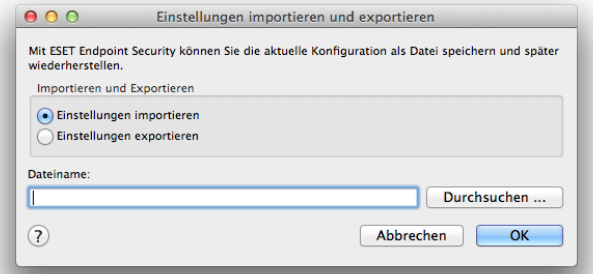
Das Benachrichtigungsfenster zeigt die vom Befehlszeilenwerkzeug 'softwareupdate' abgerufenen Updates an. Die von diesem Werkzeug abgerufenen Updates können sich von den in der Anwendung 'Software Updates' angezeigten Updates unterscheiden. Wenn Sie alle im Fenster 'Fehlende Systemupdates' angezeigten, verfügbaren Updates installieren möchten, einschließlich der nicht in der Anwendung 'Software Updates' angezeigten Updates, verwenden Sie das Befehlszeilenwerkzeug 'softwareupdate'. Weitere Informationen zu diesem Werkzeug finden Sie im Handbuch zu 'softwareupdate', auf das Sie durch Eingabe des Befehls `man softwareupdate` in einem **Terminal**fenster zugreifen können. Wir empfehlen die Nutzung des Werkzeugs nur für fortgeschrittene Benutzer.

# 14. Allgemein

## 14.1 Einstellungen importieren/exportieren

Um eine vorhandene Konfiguration zu importieren oder die aktuelle Konfiguration von ESET Endpoint Security zu exportieren, klicken Sie auf **Einstellungen** > **Einstellungen importieren und exportieren**.

Diese Funktionen sind nützlich, wenn Sie die aktuelle Konfiguration von ESET Endpoint Security für eine spätere Verwendung sichern möchten. Die Exportfunktion bietet sich auch für Benutzer an, die ihre bevorzugte Konfiguration von ESET Endpoint Security auf mehreren Systemen verwenden möchten. Sie können die Konfigurationsdatei einfach importieren, um ihre gewünschten Einstellungen zu übertragen.




### 14.1.1 Einstellungen importieren

Um eine Konfiguration zu importieren, klicken Sie im Hauptmenü auf **Einstellungen** > **Einstellungen importieren/exportieren** und anschließend auf **Einstellungen importieren**. Klicken Sie auf **Durchsuchen**, um nach der zu importierenden Konfigurationsdatei zu suchen.

### 14.1.2 Einstellungen exportieren

Um eine Konfiguration zu exportieren, klicken Sie im Hauptmenü auf **Einstellungen** > **Einstellungen importieren/exportieren** und anschließend auf **Einstellungen exportieren**. Suchen Sie mithilfe des Browsers einen Speicherort auf Ihrem Computer aus, an dem Sie die Konfigurationsdatei speichern möchten.

## 14.2 Einstellungen für den Proxyserver

Um Einstellungen für den Proxyserver zu konfigurieren, klicken Sie auf **Einstellungen** > **Erweiterte Einstellungen** > **Proxyserver**. Durch Angabe eines Proxyservers auf dieser Ebene legen Sie globale Proxyserver-Einstellungen für alle Funktionen von ESET Endpoint Security fest. Die hier definierten Parameter werden von allen Modulen verwendet, die eine Verbindung zum Internet erfordern. ESET Endpoint Security unterstützt die Authentifizierungsarten „Basic Authentication“ und „NTLM“ (NT LAN Manager).

Um die Proxyserver-Einstellungen für diese Ebene festzulegen, aktivieren Sie das Kontrollkästchen **Proxyserver verwenden** und geben im Feld **Proxyserver** die entsprechende IP-Adresse bzw. URL ein. Im Feld **Port** können Sie den Port angeben, über den Verbindungen auf dem Proxyserver eingehen (standardmäßig 3128).

Wenn für die Kommunikation mit dem Proxyserver eine Authentifizierung erforderlich ist, geben Sie in den Feldern **Benutzername** und **Passwort** die entsprechenden Informationen ein.

### 14.3 Freigegebener lokaler Cache

Um die Verwendung des freigegebenen lokalen Cache zu aktivieren, klicken Sie auf „Einstellungen“ > „Erweiterte Einstellungen“ > „Freigegebener lokaler Cache“ und aktivieren Sie das Kontrollkästchen neben „Cache mit freigegebenem lokalen ESET-Cache aktivieren“. Diese Funktion steigert die Leistung in virtualisierten Umgebungen, indem doppelte Scans im Netzwerk vermieden werden. Somit wird jede Datei nur einmal gescannt und im gemeinsamen Cache gespeichert. Wenn die Funktion aktiviert ist, werden Informationen zu den gescannten Dateien und Ordnern im Netzwerk in einem lokalen Cache gespeichert. Bei der Durchführung eines neuen Scans sucht ESET Endpoint Security nach gescannten Dateien im Cache. Wenn übereinstimmende Dateien gefunden werden, werden diese vom Scan ausgeschlossen.

Die Einstellungen für den freigegebenen lokalen Cache umfassen Folgendes:

- **Serveradresse** - Name oder IP-Adresse des Computers, auf dem sich der Cache befindet.
- **Port** - Portnummmer für die Kommunikation (standardmäßig 3537)
- **Passwort** - Passwort für den freigegebenen lokalen Cache (optional)

**HINWEIS:** Ausführliche Anweisungen zur Installation und Konfiguration des freigegebenen lokalen ESET-Cache finden Sie im ESET Shared Local Cache user guide (Benutzerhandbuch für den freigegebenen lokalen ESET-Cache). (Dieses Handbuch ist nur auf Englisch verfügbar.)